Unidad didáctica 5

El documento de seguridad

Contenido

1. Introducción

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD), establece en su punto 1 que "el Responsable del fichero y en su caso, el Encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El Título VIII del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (BOE 17, de 19 de enero de 2008) (RLOPD) desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal. El citado Título, tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad, que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Con el objeto, de facilitar a los responsables la adopción de las disposiciones del RLOPD, la Agencia Española de Protección de Datos pone a su disposición este documento, en el que se recopila un cuadro resumen de las medidas de seguridad recogidas en el citado Título VIII, un modelo de "Documento de Seguridad", que pretende servir de guía, y facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos.

AVISO IMPORTANTE

Debe entenderse, en cualquier caso, que siempre habrá que atenerse a lo dispuesto en la LOPD, en el RLOPD y en el resto de previsiones relativas a la protección de datos de carácter personal y que la utilización de este modelo como guía de ayuda para desarrollar un "Documento de Seguridad" debe, en todo caso, tener en cuenta los aspectos y circunstancias aplicables en cada caso concreto, sin prejuzgar el criterio de la Agencia Española de Protección de Datos en el ejercicio de sus funciones.

2. Guía modelo del documento de seguridad

2.1. Organización de la guía

El RLOPD especifica que se puede disponer de un solo documento, que incluya todos los ficheros y tratamientos con datos personales, de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida. En este caso se ha optado por el primer tipo, organizando el "Documento de Seguridad" en dos partes: en la primera, se recogen las medidas que afectan a todos los sistemas de información, de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye un anexo por cada fichero o tratamiento, con las medidas que le afecten de forma concreta. Además, se ha especificado aquellas medidas que afectan sólo a ficheros automatizados y las que afectan a los no automatizados de forma exclusiva.

El modelo se ha redactado, con el objeto de recopilar las exigencias mínimas establecidas por el Reglamento. Es posible y recomendable, incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

Dentro del modelo se utilizarán los siguientes símbolos convencionales:

<Comentario explicativo>:

> Entre los caracteres " <" y ">", se encuentran los comentarios aclaratorios sobre el contenido que debe tener un campo. Estos textos, no deben figurar en el documento final y deben desarrollarse para ser aplicados a cada caso concreto.

- NIVEL MEDIO. Con esta marca se señalarán las medidas, que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad medio.
- NIVEL ALTO. Con esta marca se señalarán las medidas, que sólo son obligatorias en los ficheros que tengan que adoptar un nivel de seguridad alto.
- A. Con esta marca se señalarán las medidas específicas, para aplicar exclusivamente a ficheros informatizados o automatizados.
- M. Con esta marca se señalarán las medidas específicas, para aplicar exclusivamente a ficheros manuales o no automatizados.

Las medidas, que no van precedidas de ninguna de estas marcas deben aplicarse con carácter general, tanto a ficheros o tratamientos automatizados como no automatizados, y con independencia del nivel de seguridad correspondiente.

Nota aclaratoria

Las medidas de seguridad de nivel básico, son exigibles en todos los casos. Las medidas de nivel medio, complementan a las anteriores en el caso de ficheros clasificados en este nivel y las nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.

2.2. Documento de seguridad

El Documento de Seguridad y sus Anexos, están redactados en cumplimiento de lo dispuesto en el RLOPD, y recogen las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad, de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

El contenido principal de este documento queda estructurado como sigue:

a. Ámbito de aplicación del documento.
b. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

c. Procedimiento general de información al personal.
d. Funciones y obligaciones del personal.
e. Procedimiento de notificación, gestión y respuestas ante las incidencias.
f. Procedimientos de revisión.
g. Consecuencias del incumplimiento del Documento de Seguridad.

Anexo I. Aspectos específicos relativos a los diferentes ficheros

A. Aspectos relativos al fichero <nombre del fichero a>
B. Aspectos relativos al fichero <nombre del fichero b>

Anexo II. Nombramientos

Anexo III. Autorizaciones firmadas para la salida o recuperación de datos

Anexo IV. Inventario de soportes <si se gestiona en papel>

Anexo V. Registro de incidencias <si se gestiona en papel>

Anexo VI. Contratos o cláusulas de encargados de tratamiento <Si existen, de acuerdo con lo indicado en el artículo 12 de la LOPD>

*Anexo VII. Registro de entrada y salida de soporte*s

Este documento deberá mantenerse permanente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

a. Ámbito de aplicación del documento

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de <nombre del responsable>, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser

protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

NIVEL ALTO**.** Se aplicarán a los ficheros o tratamientos de datos:

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

NIVEL MEDIO. Se aplicarán a los ficheros o tratamientos de datos:

- Relativos a la comisión de infracciones administrativas o penales.
- Que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito).
- De las Administraciones tributarias y que se relacionen con el ejercicio de sus potestades tributarias.
- De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros.
- De entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias.
- De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.
- De los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización. (Para esta última categoría de ficheros además deberá disponerse de un registro de accesos).

NIVEL BÁSICO. Se aplicarán a cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.
- Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

<Incluir relación de ficheros o tratamientos afectados, indicando si se trata de sistemas automatizados, manuales o mixtos y el nivel de seguridad que les corresponde>.

En el Anexo I de este documento se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

Caso práctico-empresa A

En este primer caso, vamos a mostrar el ejemplo de cómo quedaría redactado este apartado dentro del correspondiente Documento de Seguridad perteneciente a nuestra primera empresa "LOPD Comunicaciones S.L." Dicho documento estaría elaborado por el Responsable del fichero, que en este caso sería Pablo García García, y su cumplimiento sería obligado para el resto del personal que trabaja en la empresa. Veamos cómo habría quedado redactado el mencionado apartado.

Ámbito de aplicación

Este documento, será de aplicación a los ficheros que contienen datos de carácter personal, que se hallan bajo la responsabilidad de Pablo García García, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento con indicación del nivel de seguridad correspondiente, son los siguientes:

- **"Fichero _clientes" (Fichero con los datos personales de los clientes de la empresa). Nivel de seguridad básico**

En el Anexo I se describe detalladamente junto con los aspectos que le afecten de manera particular.

Caso práctico-empresa B

En este segundo ejemplo, vamos a describir cómo quedaría realizado el mencionado apartado dentro del Documento de Seguridad perteneciente a la empresa de seguros "LOPD SEGUROS S.L.", antes de que se decidiera la incorporación de datos relativos a la salud de los clientes.

Ámbito de aplicación

Este documento, será de aplicación a los ficheros que contienen datos de carácter personal, que se hallan bajo la responsabilidad de Antonio Pérez Pérez, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento con indicación del nivel de seguridad correspondiente, son los siguientes:

- **"Fichero_clientes". Nivel de seguridad medio**

  En el Anexo I se describe detalladamente, junto con los aspectos que le afecten de manera particular.

  Además del fichero automatizado, existe un fichero manual o no automatizado que es el:

- **"Fichero_ Otra documentación de los clientes". Nivel de seguridad alto**

  Como explicamos en el tema 2, en este fichero aparecen no sólo datos de nivel medio sino también datos de carácter personal referentes a la salud de los clientes que contratan un seguro, como son los partes médicos, por lo tanto estos datos necesitan de una especial protección y se les aplicarán las medidas de nivel alto.

Caso práctico-empresa C

Veamos, en este tercer supuesto cómo habría quedado el correspondiente apartado del Documento de Seguridad de la clínica "LOPD ODONTOS S.L.", el cual habría sido redactado por Fernando Ruiz Ruiz, dueño de la clínica y responsable del tratamiento.

A

Ámbito de aplicación

Este documento, será de aplicación a los ficheros que contienen datos de carácter personal, que se hallan bajo la responsabilidad de Fernando Ruiz Ruiz, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

- **"Fichero _Ficha Pacientes". Nivel de seguridad Básico**
- **"Fichero _Datos Clínicos". Nivel de seguridad alto**

En el Anexo I, se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

Existe un fichero manual o no automatizado, "Fichero pruebas clínicas" que contiene datos de carácter personal, entre ellos existen datos relativos a la salud, como las pruebas radiológicas o las analíticas, por lo tanto se le aplicarían las medidas seguridad de nivel alto que establece este documento.

B. Medidas, normas procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento

Identificación y Autenticación

Medidas y normas, relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales.

A

<Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales. La identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización (cada identificación debe pertenecer a un único usuario).

Si la autenticación se realiza mediante contraseñas, detallar el procedimiento de asignación, distribución y almacenamiento que deberá garantizar su confidencialidad e integridad e indicar la periodicidad con la que se deberán cambiar, en ningún caso superior a un año.

También es conveniente, incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña>.

A

NIVEL MEDIO

En los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Control de acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El Responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados <incluir estos mecanismos>.

Exclusivamente el <persona autorizada (o denominación de su puesto de trabajo) para conceder, alterar o anular el acceso autorizado> está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, conforme a criterios establecidos por el Responsable del fichero <nota: si la persona es diferente en función del fichero, incluir el párrafo en la parte del Anexo I correspondiente>.

<Especificar los procedimientos para solicitar el alta, modificación y baja de las autorizaciones de acceso a los datos, indicando que persona (o puesto de trabajo) concreta tiene que realizar cada paso.

Incluir y detallar los controles de acceso a los sistemas de información>.

En el Anexo I se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará <Especificar procedimiento de actualización>.

De existir personal ajeno al Responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

A

NIVEL MEDIO. CONTROL DE ACCESO FÍSICO

Exclusivamente el personal que se indica a continuación, podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información correspondientes a < indicar los nombres de los ficheros de nivel medio y alto>.

NIVEL ALTO. REGISTRO DE ACCESOS

A

En los accesos a los datos, de los ficheros de nivel alto. <indicar los nombres de los ficheros de nivel alto.> se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

<Indicar si se estima oportuno, información relativa al sistema de registro de accesos. El mecanismo que permita este registro estará bajo control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación del mismo>.

Los datos del registro de accesos, se conservaran durante< especificar periodo, que deberá ser al menos de dos años. No es preciso que estos datos se almacenen "on line">.

El responsable de seguridad, revisará al menos una vez al mes la información de control registrada, y elaborará un informe según se detalla en el Capítulo VI de este documento.

No será necesario el registro de accesos cuando:

- El Responsable del fichero es una persona física.
- El Responsable del fichero garantice que sólo él tiene acceso y trata los datos personales.
- Se haga constar en el Documento de Seguridad.

M

El acceso a la documentación, se limita exclusivamente al personal autorizado.

Se establece el siguiente mecanismo, para identificar los accesos realizados en el caso de los documentos relacionados< indicar los documentos o tipos de documentos que puedan ser utilizados por múltiples usuarios, así como el mecanismo establecido para controlar estos accesos; igualmente se definirá en este punto un registro de accesos general>.

Gestión de soportes y documentos

Los soportes que contengan datos de carácter personal, deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en <indicar el lugar de acceso restringido donde se almacenarán> un lugar de acceso restringido, al que solo tendrán acceso las personas con autorización que se relacionan a continuación: <Especificar el personal autorizado a acceder al lugar donde se almacenan los soportes que contengan datos de carácter personal, el procedimiento a seguir para habilitar o retirar el permiso de acceso. Tener en cuenta, el procedimiento a seguir para casos en que personal no autorizado tenga que tener acceso a los locales, por razones de urgencia o fuerza mayor>.

Los siguientes soportes, <relacionar aquellos a que se refiere > cumplirán con las obligaciones indicadas en el párrafo anterior, dadas sus características físicas, que imposibilitan el cumplimiento de las mismas.

Los siguientes soportes, <indicar aquellos que contengan datos considerados especialmente sensibles y respecto de los que se haya optado por proceder del siguiente modo> se identificarán utilizando sistemas de etiquetado siguientes < especificar, los criterios de etiquetado que serán comprensibles y con significado para los usuarios autorizados, permitiéndoles identificar su contenido y que sin embargo dificultan la identificación para el resto de personas>.

Los soportes, se almacenarán de acuerdo a las siguientes normas: < indicar normas de etiquetado de los soportes. Especificar el procedimiento

de inventariado y almacenamiento de los mismos. El inventario de soportes, puede anexarse al documento o gestionarse de forma automatizada, en este último caso se indicará en este punto el sistema informático utilizado>.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el Responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento <detallar el procedimiento a seguir para que se lleve a cabo la autorización. Tener en cuenta también los ordenadores portátiles y el resto de dispositivos móviles que puedan contener datos personales>.

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente <detallar procedimiento a realizar para su destrucción o borrado> de forma que no sea posible el acceso a la información contenida en ello o su recuperación posterior.

En el traslado de la documentación se adoptarán las <indicar medidas y procedimientos previstos> para evitar la sustracción, pérdida o acceso indebido a la información.

A

NIVEL MEDIO. REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Las salidas y entradas de soportes correspondientes a los ficheros< indicar los nombres de los ficheros de nivel medio y alto>, deberán ser registradas de acuerdo al siguiente procedimiento: <Detallar el procedimiento por el que se registrarán las entradas y salidas de soportes>.

El registro de entrada y salida de soportes, se gestionará mediante <indicar la forma en que se almacenará el registro, que ser manual o informático> y en

el que deberán constar < indicar los campos del registro, que deberán ser, al menos, en el caso de las entradas, el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción y en el caso de las salidas, el tipo de documento o soporte, la fecha y la hora, el destinatario, el número de documentos o soporte incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega>.

<En caso de gestión automatizada, se indicará en este punto el sistema informático utilizado>.

A

NIVEL ALTO. GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

Los soportes relacionados <indicar aquellos de nivel alto> serán identificados mediante el sistema de etiquetado <especificar los criterios de etiquetado que resultarán comprensibles y con significado para los usuarios con acceso autorizados, permitiéndoles identificar su contenido y dificultando la identificación para el resto de personas>.

La distribución y salida de soportes que contengan datos de carácter personal de los ficheros <indicar los nombres de los ficheros de nivel alto> se realizará < indicar el procedimiento para cifrar los datos o, en su caso, para utilizar el mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. Igualmente se cifrarán los datos que contengan los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable>.

Los siguientes dispositivos portátiles <relacionar aquellos que no permitan el cifrado de los datos personales>, serán utilizados en el tratamiento de datos personales adoptándose las medidas que a continuación se explicitan < relacionar las medidas alternativas que tendrán en cuenta los riesgos de realizar tratamientos en entornos desprotegidos>.

M

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios <indicar los previstos en la legislación que les afecte o en su defecto, los establecidos por el Responsable del fichero, que en cualquier caso deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación>.

M

ALMACENAMIENTO DE LA INFORMACIÓN

Los siguientes dispositivos <relacionarlos así como aquellas de sus características que obstaculicen su apertura. Cuando sus características físicas no permitan adoptar esta medida, el responsable adoptará medidas que impidan el acceso a la información de personas no autorizadas> serán utilizados para guardar los documentos con los datos personales.

NIVEL ALTO

Los elementos de almacenamiento <indicar tipos como armarios, archivadores u otros elementos utilizados> respecto de los documentos con datos personales, se encuentran en <indicar lugares físicos y protección con que cuenta el acceso a las mismas, como llaves u otros dispositivos. Además estos lugares permanecerán cerrados en tanto no sea preciso el acceso a los documentos. Si a la vista de las características de los locales no fuera posible cumplir lo anteriormente indicado, se adoptarán medidas alternativas que se reflejarán en este punto>.

M

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamientos indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren al cargo de los mismos deberán custodiarlos e impedir en todo momento que pueda ser accedida por personas no autorizadas.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

<Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Relacionar los accesos previstos y los ficheros a que se prevea acceder>.

A

NIVEL ALTO. Los datos personales correspondientes a los ficheros< relacionar los de nivel alto>, que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos < indicar en su caso otros mecanismos distintos del cifrado que se utilicen y que garanticen que la información no sea inteligible ni manipulada por terceros. También podría ser adecuado cifrar los datos en red local>.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se pueden llevar a cabo los siguientes tratamientos de datos personales <relacionar los ficheros a que afecten estos tratamientos> fuera de los locales de este Responsable del fichero <indicar en su caso, los distintos locales a los que se deban circunscribir dichos tratamientos, especialmente en el supuesto de que se produzcan tratamientos por un Encargado del tratamiento que se especificará>, así como mediante dispositivos portátiles. Esta autorización regirá durante <indicar el período de validez de la misma>.

<Esta autorización puede realizarse para unos usuarios concretos que habría que indicar o para un perfil de usuarios>.

<Se debe garantizar el nivel de seguridad correspondiente al fichero tratado en dichos tratamientos>.

M

TRASLADO DE DOCUMENTACIÓN

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las siguientes medidas <relacionar las de necesaria utilización siempre que sea posible y en su caso alternativas recomendadas, orientadas a impedir el acceso o manipulación de la información objeto de traslado>.

FICHEROS TEMPORALES

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de Seguridad y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

M

COPIA O REPRODUCCIÓN

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del siguiente personal autorizado <indicar los usuarios o perfil de los mismos habilitados para ello>.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida en las mismas <indicar los medios a utilizar o puestos a disposición de los usuarios para ello>.

A

COPIAS DE SEGURIDAD

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad <especificarla y en todo caso será como mínimo una vez a la semana>.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente respecto de los ficheros parcialmente automatizados siguientes <indicarlos>, se grabarán manualmente los datos. <Para la grabación manual indicada deberá existir documentación que permita dicha reconstrucción>.

El Responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos personales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

NIVEL ALTO

En los ficheros <indicar ficheros de nivel alto> se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en <especificar el lugar, diferente de donde se encuentran los sistemas informáticos que los tratan y que deberá cumplir las medidas de seguridad o utilizando elementos que garanticen la integridad y recuperación de la información de forma que sea recuperable>.

NIVEL MEDIO. RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad <indicarlo/os en el caso de que se prevea que sean varios>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este Documento de Seguridad. <La designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento, lo que se especificará en este documento, en la parte correspondiente del Anexo I>.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a <denominación Responsable del fichero o del Encargado del tratamiento> como Responsable del fichero de acuerdo con el Reglamento de desarrollo de la LOPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de <indicar periodo de desempeño del cargo>. Una vez transcurrido este plazo <denominación Responsable del fichero> podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

Supuestos específicos sobre las copias de seguridad referentes a los supuestos de las tres empresas: empresa A, empresa B, y empresa C.

Caso práctico -empresa A

Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal, salvo que no se hubiese producido ninguna actualización de los datos y si no se especifica la periodicidad será como mínimo una vez a la semana. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos personales previa copia de seguridad y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Recuperación de datos

El Responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de datos.

En el Anexo III se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

Caso práctico - empresa B

Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En los ficheros manuales se grabarán manualmente los datos. Para la grabación manual deberá existir documentación que permita dicha reconstrucción.

El Responsable del fichero verificará semestralmente los procedimientos de copias de recuperación de los datos.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Ejemplo

Recuperación de datos
Las recuperaciones de datos del fichero "fichero_clientes" deberán ser autorizadas por el Responsable del fichero según el procedimiento indicado en el capítulo correspondiente.

En el Anexo III se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

Caso práctico - empresa C

Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción, en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Ejemplo

En el fichero "fichero_Datos clínicos" se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en el domicilio personal de Fernando Ruiz Ruiz, además de la que se guarda en la propia clínica. Por ello, las copias de respaldo se realizarán por duplicado.

En el fichero "fichero_otras pruebas clínicas" se grabarán manualmente los datos. Para la grabación manual deberá existir documentación que permita su reconstrucción.

Recuperación de datos

En el anexo se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

Ejemplo

Las recuperaciones de datos del fichero "fichero_Datos clínicos" deberán ser autorizadas por escrito por el Responsable del fichero.

Caso práctico-empresa A

Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales.

Los usuarios accederán al sistema mediante la introducción de un identificador de usuario y una clave que tendrán asignados desde el momento de alta en el sistema.

El Responsable del fichero es el único con competencia para conceder, alterar o anular los accesos autorizados a los sistemas.

Cada uno de los usuarios estará asignado a un perfil, de manera que exclusivamente tenga acceso autorizado a los recursos que precisa para desempeñar su función.

Cada acceso autorizado a los Sistemas de Información, deberá estar identificado unívocamente con el usuario correspondiente.

La generación de altas y bajas de usuario, así como la modificación de derechos de acceso de los usuarios, se tramitarán mediante el siguiente procedimiento de administración de usuarios.

Las contraseñas las asigna el Responsable del fichero cuando da de alta a un nuevo usuario. Esta contraseña es entregada por escrito al usuario en un sobre cerrado para su consulta privada. Una vez que un usuario accede por primera vez al sistema, lo primero que debe hacer es cambiar su contraseña de acceso que quedará almacenada en el sistema de forma cifrada. Las contraseñas deben ser modificadas por los usuarios cada 360 días. La longitud mínima para una contraseña será de 6 caracteres alfanuméricos y se obliga a no utilizar palabras que puedan contener algún significado.

De cualquier modo, existirá un registro actualizado de los usuarios con acceso autorizado al Sistema de Información al que sólo tendrá acceso el Responsable del fichero. Este registro estará contenido en un fichero de Excel llamado "usuario.xls". Dicho registro de usuarios contendrá la siguiente información:

- Nombre del usuario.
- Cargo que desempeña en la empresa.
- Identificador de usuario.
- Perfil de usuario.

Cada vez que se produzca el alta o baja de un usuario en el sistema, el Responsable del fichero revisará el registro de usuarios y lo actualizará con el alta o baja que se haya producido.

CONTROL DE ACCESO

Los clientes sólo podrán entrar en la tienda en horario de apertura al público. El resto del tiempo la tienda estará cerrada al público. Además, cualquier ordenador de la tienda se situará tras un mostrador que impida su acceso al público.

Todos los usuarios del sistema velarán para que su puesto de trabajo no quede accesible a otra persona. Si un usuario debe ausentarse de su puesto dejará la sesión bloqueada con contraseña para que nadie pueda aprovechar la ocasión y acceder al sistema.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.

Exclusivamente, el Responsable del fichero (Pablo) está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

El Responsable del fichero (Pablo) será quien se encargue de dar de alta, modificar o dar de baja las autorizaciones de acceso a los datos, mediante la incorporación de nuevos usuarios en el sistema y su asignación o modificación de un perfil de usuario. Todos los usuarios que se creen tendrán como contraseña predeterminada la asignada por Pablo, que será notificada al usuario en un sobre cerrado.

En el Anexo I se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará cada vez que se cree un nuevo usuario.

GESTIÓN DE SOPORTES. REGISTRO DE ENTRADA Y SALIDA

Los soportes que contengan datos de carácter personal deben permitir su identificación, inventariado y almacenamiento en un armario cerrado con llave, lugar de acceso restringido.El armario tiene una hoja de accesos en la puerta. Cada vez que se abra el armario se anotará la fecha y hora en la hoja, además del soporte accedido o añadido.

Ejemplo

A este lugar sólo tendrán acceso las personas con autorización que se relacionan a continuación:

- Pablo García García: Tiene su propia llave.
- Juan López López: Necesita pedir la llave a Pablo.
- José Pérez García: Necesita pedir la llave a Pablo.
- María Dolores Jiménez Ruiz: Necesita pedir la llave a Pablo.
- Personal no autorizado (por fuerza mayor): Solicitaría la llave a Pablo.

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas:

- Se almacenará con una etiqueta que indique la fecha de grabación del soporte. Dentro del armario estarán ordenados por orden de fechas. El inventario de soportes actual sería el siguiente:

  - CD1. Clientes- Enero- 2006.
  - CD2. Clientes- Febrero- 2006.
  - CD3. Clientes-Marzo- 2006.

La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser autorizada por el Responsable del fichero o aquel en

que se hubiera delegado de acuerdo al siguiente procedimiento: Pablo dará su autorización por escrito y dicha autorización se anotará en un registro de entrada/ salida. En el anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Se deberá indicar relación de accesos previstos y los ficheros a los que se prevea acceder.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se puede llevar a cabo el tratamiento de datos personales fuera de los locales de este Responsable del fichero cuando se indique la relación de ficheros a los que afecten estos tratamientos, además de indicar los locales a los que se deban circunscribir dichos tratamientos, especialmente cuando dichos tratamientos se produzcan por un Encargado del tratamiento. También habrá de indicarse el período de validez para llevar a cabo esta tarea y determinar qué usuarios pueden desempeñar esta función.

En el supuesto que se les plantea no se prevé el tratamiento de datos fuera del Responsable del fichero (Pablo), es decir, los tratamientos sólo serán ejecutados en las instalaciones de la empresa.

FICHEROS TEMPORALES

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el reglamento (en este supuesto el nivel de seguridad que les corresponde es el básico) y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

COPIAS DE SEGURIDAD

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del Responsable del fichero (Pablo). La persona con acceso autorizado para la realización de copias o reproducción de documentos será José.

Las copias desechadas deberán ser destruidas, imposibilitando el posterior acceso a la información contenida en las mismas. Por esta razón, se deben indicar los medios puestos a disposición de los usuarios para ello.

Se realizarán copias de respaldo salvo que no se hubiese producido ninguna actualización de los datos diariamente. Si esto no fuera posible, se realizará como mínimo una vez a la semana.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

El Responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos personales previa copia de seguridad y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Caso práctico-empresa B

Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales

Antes de comentar cuáles son estas medidas y normas debemos recordar que nuestra empresa contaba además de con un fichero automatizado

con un manual, al cual haremos alusión más tarde. Ahora vamos a contarles cuáles son las medidas que se van aplicar al fichero automatizado.

Cada usuario accederá al sistema mediante la introducción de un identificador de usuario y una clave.

El Responsable del fichero es el único con competencia para conceder, alterar o anular los accesos autorizados a los sistemas.

Cada uno de los usuarios estará asignado a un perfil, de manera que exclusivamente tenga acceso autorizado a los recursos que precisa para desempeñar su función. Cada acceso autorizado a los Sistemas de Información deberá estar identificado unívocamente con el usuario correspondiente.

La generación de altas y bajas de usuario y la modificación de derechos de acceso de los usuarios se tramitarán mediante el siguiente procedimiento de administración de usuarios:

- Las contraseñas las asigna el Responsable del fichero cuando da de alta a un nuevo usuario. Esta contraseña es entregada por escrito al usuario en un sobre cerrado para su consulta privada. Una vez que un usuario accede por primera vez al sistema, lo primero que debe hacer es cambiar su contraseña de acceso que quedará almacenada en el sistema de forma cifrada. Las contraseñas deben ser modificadas por los usuarios cada 360 días. La longitud mínima para una contraseña será de 6 caracteres alfanuméricos y se obliga a no utilizar palabras que puedan contener algún significado.
  De cualquier modo, existirá un registro actualizado de los usuarios con acceso autorizado para el Sistema de Información, al que sólo tendrá acceso el Responsable del fichero. Este registro estará contenido en un fichero de Excel llamado "usuario.xls". Dicho registro de usuarios contendrá la siguiente información:
- Nombre del usuario.
- Cargo que desempeña en la empresa.
- Identificador de usuario.
- Perfil de usuario.

Cada vez que se produzca el alta o baja de un usuario en el sistema, el Responsable del fichero revisará el registro de usuarios y lo actualizará con el alta o baja que se haya producido.

Ejemplo

Control de acceso
En el fichero "fichero_ clientes" la identificación de los usuarios se deberá realizar de forma inequívoca y personalizada verificando su autorización. (Cada identificación debe pertenecer a un único usuario). Asimismo, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Además, en los ficheros se deberán indicar los nombres de los ficheros de nivel medio y alto.

Los clientes sólo podrán entrar en las dependencias en horario de apertura al público. El resto del tiempo la empresa estará cerrada al público. Además, los ordenadores de la empresa se situarán tras mostradores o mamparas que impidan su acceso al público.

Todos los usuarios del sistema velarán para que el puesto de trabajo no quede accesible a otra persona. Si un usuario debe ausentarse de su puesto dejará la sesión bloqueada con contraseña para que nadie pueda aprovechar la ocasión y acceder al sistema.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.

Exclusivamente el Responsable del fichero, Antonio Pérez Pérez, está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

El Responsable del fichero (Antonio) será quien se encargue de dar el alta, modificar o dar de baja las autorizaciones de acceso a los datos mediante la incorporación de nuevos usuarios en el sistema y su asignación o modificación

de un perfil de usuario. Todos los usuarios que se crean tienen como contraseña predeterminada la que el Responsable del fichero le asigne en ese momento y que será entregada por escrito al nuevo usuario. En el Anexo I se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará cada vez que se cree o se borre un usuario.

Ejemplo

Control de acceso físico
Exclusivamente, el personal que se indica a continuación podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información correspondientes a "fichero_clientes".

- Antonio Pérez Pérez: Gerente de la empresa.
- María López López: Abogada.
- Pedro Jiménez Jiménez: Economista.

GESTIÓN DE SOPORTES

Los soportes que contengan datos de carácter personal deben permitir su identificación, ser inventariados y almacenados en la habitación de soportes, lugar de acceso restringido al que sólo tendrán acceso las personas con autorización que se relacionan a continuación:

- Antonio Pérez Pérez.
- María López López.
- Pedro Jiménez Jiménez.

Para acceder a la habitación de soportes, los usuarios rellenarán y firmarán un formulario con los datos del acceso (fecha hora, soporte accedido) y lo registrarán en el sistema mediante su escritura en un archivo de Word llamado "accesos.doc", el cual contiene el historial de accesos a los soportes almacenados.

Para el acceso de otra persona ajena a la empresa se requiere la autorización de Antonio, quien dará dicha autorización, la firmará y registrará junto con los datos del acceso en el mismo fichero "accesos.doc".

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas:

- Cada soporte llevará una etiqueta adhesiva que contendrá la fecha de grabación y el tipo de datos que contiene, así como el tipo de copia (incremental, diferencial, diaria, etc.) Dentro de la habitación los soportes estarán ordenados por fecha de grabación. La lista con los soportes existentes se encuentra escrita en un fichero de Excel llamado "soportes.xls", el cual es actualizado o modificado por Antonio, cada vez que se incorpora o elimina un soporte.
- La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser autorizada por el Responsable del fichero (Antonio) o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento: La persona en cuestión solicitará la autorización a Antonio, el cual la dará firmada por escrito. Una vez dada dicha autorización el Responsable del fichero la registrará en un fichero de Excel llamado "salidas.xls" que contendrá los datos de la persona que solicita la salida, la fecha y la hora de salida, el nombre y descripción del soporte que se lleva. En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Registro de entrada y salida de soportes

Las salidas y entradas de soportes correspondientes al fichero "ficheros_clientes" deberán ser registradas de acuerdo al siguiente procedimiento:

El Responsable del fichero dará su autorización escrita y firmada para la salida o entrada de soportes y la registrará en el fichero de Excel correspondiente "entradas.xls" o "salidas.xls".

El registro de entrada y salida de soportes se gestionará mediante su edición utilizando la herramienta ofimática Microsoft Excel 2000 y en el que deberán constar:

- Para entradas: tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción.
- Para las salidas: el tipo de documento o soporte, la fecha y la hora, el destinatario, el número de documentos o soporte incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega.

El fichero se encuentra en el ordenador de Antonio, el cual tiene implantado Windows XP y MS Office 2000.

Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal, a través de redes de comunicaciones, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Se deberá indicar la relación de accesos previstos y los ficheros a los que se prevean acceder.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se puede llevar a cabo el tratamiento de datos personales fuera de los locales de este Responsable del fichero cuando se indique la relación de ficheros a los que afecten estos tratamientos, además de indicar los locales a los que se deba circunscribir dichos tratamientos, especialmente cuando dichos tratamientos se produzcan por un Encargado del tratamiento. También habrá de indicarse el período de validez para llevar a cabo esta tarea y determinar qué usuarios pueden desempeñar esta función.

En el supuesto que se plantea, no se prevé el tratamiento de datos fuera del Responsable del fichero (Pablo), es decir, los tratamientos sólo serán ejecutados en las instalaciones de la empresa.

FICHEROS TEMPORALES

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el reglamento (en este supuesto el nivel de seguridad que les corresponde es el básico) y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

COPIAS DE SEGURIDAD

La realización de copias o reproducción de los documentos con datos personales, sólo se podrán realizar bajo el control del Responsable del fichero (Pablo). La persona con acceso autorizado para la realización de copias o reproducción de documentos será Pedro.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida en las mismas, por esta razón se deben indicar los medios puestos a disposición de los usuarios para ello.

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos diariamente (si esto no fuera posible, se realizará como mínimo una vez a la semana).

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

El Responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos personales previa copia de seguridad y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Ejemplo

María López López, con carácter general, se encargará de coordinar y controlar las medidas definidas en este Documento de Seguridad.

En ningún caso la designación supone una delegación de la responsabilidad que corresponde a Antonio Pérez Pérez, como Responsable del fichero de acuerdo con el reglamento.

El responsable de seguridad desempeñará las funciones durante el periodo de 2012. Una vez transcurrido este plazo, Antonio Pérez Pérez podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

Recordamos que esta empresa también contaba con un fichero manual "fichero_ otra documentación de clientes".

- El acceso a la documentación se limita exclusivamente al personal autorizado. Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados:

  - Identificador. Código de registro.
  - Nombre: fichero_clientes.
  - Descripción. Fichero con los datos personales de los clientes que contratan algún tipo de póliza de seguros.
    El personal autorizado sería (Antonio), (María), (Pedro).

- Los criterios de archivo se realizarán de acuerdo con la legislación que le afecte, o en su defecto, los establecidos por el Responsable del fichero que en cualquier caso deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
- Almacenamiento de la información.
  Los elementos de almacenamiento, como armarios o archivadores se encuentran en lugares protegidos y cuentan con llaves u otros dispositivos. Además estos lugares permanecerán cerrados en cuanto no sea preciso el acceso a los documentos.
- Custodia de soportes.
  Las personas que se encuentren al cargo de la custodia de soportes, deberán custodiarlos e impedir en todo momento que pueda ser accedida por personas no autorizadas.
- Traslado de documentación.
  Deberán adoptarse medidas orientadas a impedir el acceso o manipulación de la información objeto de traslado.
- Copias de reproducción.
  La realización de copias de reproducción de documentos con datos personales sólo se podrá realizar bajo el control del personal autorizado.
  Las copias desechadas, deberán ser destruidas imposibilitando el posterior acceso a la información contenida en las mismas.

Caso práctico empresa C

Medidas y normas relativas a la identificación y autentificación del personal autorizado a acceder a los datos personales

Los usuarios accederán al sistema mediante la introducción de un identificador de usuario y una contraseña.

El Responsable del fichero es el único con competencia para conceder, alterar o anular los accesos autorizados a los sistemas.

Cada uno de los usuarios estará asignado a un perfil, de manera que exclusivamente tenga acceso autorizado a los recursos que precisa para desempeñar su función.

Cada acceso autorizado a los sistemas de información deberá estar identificado unívocamente con el usuario correspondiente.

La generación de altas y bajas de usuario, así como la modificación de derechos de acceso de los usuarios se tramitarán mediante el siguiente procedimiento de administración de usuarios:

- Las contraseñas las asigna el Responsable del fichero cuando da de alta a un nuevo usuario. Esta contraseña es entregada por escrito al usuario en un sobre cerrado para su consulta privada. Una vez que un usuario accede por primera vez al sistema, lo primero que debe hacer es cambiar su contraseña de acceso, que quedaría almacenada en el sistema de forma cifrada. Las contraseñas deben ser modificadas por los usuarios cada 360 días. La longitud mínima para una contraseña será de 6 caracteres alfanuméricos y se obliga a no utilizar palabras que puedan contener algún significado.

De cualquier modo, existirá un registro actualizado de los usuarios con acceso autorizado para el sistema de información al que sólo tendrá acceso el Responsable del fichero. Este registro estará contenido en un fichero llamado "usuarios.ods" que puede ser editado mediante la aplicación ofimática Open Office.org Calc. Dicho registro de usuarios contendrá la siguiente información:

- Nombre del usuario.
- Cargo que desempeña en la empresa.
- Identificador de usuario.
- Perfil de usuario.

Cada vez que se produzca el alta o baja de un usuario en el sistema, el Responsable del fichero revisará el registro de usuarios y lo actualizará con el alta o baja que se haya producido.

Ejemplo

En el fichero "fichero_ Datos Clínicos", la identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización (cada identificación debe pertenecer a un único usuario).

Asimismo, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Control de acceso

Los clientes sólo podrán entrar en las dependencias en horario de apertura al público. El resto del tiempo, la clínica estará cerrada al publico. Además, todo ordenador de la clínica se situará tras un mostrador o mampara que impida su acceso al público.

Todos los usuarios del sistema velarán para que su puesto de trabajo no quede accesible a otra persona. Si un usuario debe ausentarse de su puesto dejará la sesión bloqueada con contraseña para que nadie pueda aprovechar la ocasión y acceder al sistema.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.

Exclusivamente el Responsable del fichero, Fernando Ruiz Ruiz, está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

El Responsable del fichero (Fernando) será quien se encargue de dar de alta, modificar o dar de baja las autorizaciones de acceso a los datos, mediante la incorporación de nuevos usuarios en el sistema y su asignación o modificación de un perfil de usuario. Todos los usuarios que se crean tienen como contraseña predeterminada la que el Responsable del fichero le asigne, entregándosela por escrito al nuevo usuario.

Cada vez que un usuario entra en el sistema se actualiza un archivo "log" que almacena cada uno de los accesos que el usuario realiza al fichero "fichero_pacientes", con indicación del dato concreto al que accede y la operación que realiza sobre sí mismo.

Este fichero sólo es accesible por el usuario administrador (en este caso Fernando) y el responsable de seguridad (Miguel).

En el Anexo I se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará cada vez que se cree o se borre un usuario.

Ejemplo

Control de acceso físico
Exclusivamente el personal que se indica a continuación podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información correspondientes a "fichero_Datos clínicos".

- Fernando Ruiz Ruiz. Odontólogo y propietario de la clínica.
- Miguel Gutiérrez Gutiérrez. Odontólogo.
- Teresa Muñoz Muñoz. Auxiliar de clínica.
- Marta Luque Luque. Auxiliar de clínica.
- Sonia Martín Martín. Auxiliar de clínica.

Ejemplo

Registro de accesos
En los accesos a los datos de los ficheros de nivel alto,"fichero_ Datos Clínicos" se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado se almacenará también la información que permita identificar el registro accedido.

Esta información quedaría guardada en un fichero "log" que se escribió de forma automática por el propio sistema de gestor de la base de datos. Dicho fichero sólo será accesible por el administrador (Fernando) y el responsable de seguridad (Miguel).

Los datos del registro de accesos se conservarán durante dos años.

El responsable de seguridad revisará periódicamente la información de control registrada y elaborará un informe según se detalla en el Capítulo VI de este documento.

Ejemplo

Gestión de soportes
Este será un lugar de acceso restringido al que sólo tendrán acceso las personas con autorización que se relacionan a continuación:

- Fernando Ruiz Ruiz
- Miguel Gutiérrez Gutiérrez
- Sonia Martín Martín

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y almacenados en una habitación especial para soportes.

Para acceder a la habitación de los soportes, los tres usuarios rellenarán y firmarán un formulario con los datos del acceso (fecha hora, soporte accedido) y lo registrarán en el sistema mediante su escritura en un archivo de Open Office.org Calc llamado "accesos.ods", el cual contiene el historial de accesos a los soportes almacenados.

Para el acceso de otra persona se requiere la autorización de Fernando, quien dará dicha autorización, la firmará y registrará con los datos del acceso en el mismo fichero "accesos.ods".

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas:

- Cada soporte llevará una etiqueta adhesiva que contendrá la fecha de grabación y el tipo de datos que contiene, así como el tipo de copia (incremental, diferencial, diaria, etc.). Dentro de la habitación los soportes estarán ordenados por fecha de grabación. La lista con los soportes existentes se encuentra escrita en un fichero de Open Office.org Calc llamado "soportes.ods", el cual es actualizado o modificado por Fernando cada vez que se incorpora o elimina un soporte.

La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser autorizada por el Responsable del fichero (Fernando) o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento:

La persona en cuestión solicitará la autorización a Fernando, el cual la dará firmada por escrito. Una vez dada dicha autorización, el Responsable del fichero la registrará en un fichero de open Office.org Calc llamado "salidas. Ods" que contendrá los datos de la persona que solicita la salida, la fecha y hora de la salida, el nombre y descripción del soporte que se lleva. En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Registro de entrada y salida de soportes

Las salidas y entradas de soportes correspondientes al "fichero_Datos clínicos" deberán ser registradas de acuerdo al siguiente procedimiento:

El Responsable del fichero dará su autorización escrita y firmada para la salida o entrada de soportes y la registrará en el fichero correspondiente "entradas.ods" o "salidas.ods".

El registro de entrada y salida de soportes se gestionará mediante su edición utilizando la herramienta ofimática "Open Office.org Calc" y en el que deberá constar:

- Para entradas. Tipo de soportes, unidades, NIF y nombre del emisor, fecha y hora de la entrega, descripción de la información, forma de envío y persona que lo recibe.
- Para salidas. Tipo de soporte, unidades, NIF y nombre del destinatario, fecha y hora de la salida, descripción de la información, forma de envío y responsable de la entrega.

El fichero se encuentra en el Sistema de información de la clínica, el cual tiene implantado Guadalinex 2004 y Open Office.org 2.0.

Ejemplo

Distribución cifrada de soportes
La distribución y salida de soportes que contengan datos de carácter personal del fichero "fichero_Datos clínicos", se realizará encriptando previamente los datos con la aplicación "Mcrypt". Una vez encriptados se procederá a grabarlos en el soporte adecuado y a registrar su salida en el fichero "salidas.ods".

Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Se deberá indicar la relación de accesos previstos y los ficheros a los que se prevea acceder.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Se puede llevar a cabo el tratamiento de datos personales fuera de los locales de este Responsable del fichero, cuando se indique la relación de ficheros a los que afecten estos tratamientos, además de indicar los locales a los que se deban circunscribir dichos tratamientos, especialmente cuando dichos tratamientos se produzcan por un Encargado del tratamiento. También habrá de indicarse el periodo de validez para llevar a cabo esta tarea y determinar qué usuarios pueden desempeñar esta función.

En el supuesto que se plantea no se prevé el tratamiento de datos fuera del Responsable del fichero (Pablo), es decir, los tratamientos sólo serán ejecutados en las instalaciones de la empresa.

FICHEROS TEMPORALES

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el reglamento (en este supuesto el nivel de seguridad que les corresponde es el básico) y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

COPIAS DE SEGURIDAD

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del Responsable del fichero (Pablo). La persona con acceso autorizado para la realización de copias o reproducción de documentos será Pedro.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida en las mismas, por esta razón se deben indicar los medios puestos a disposición de los usuarios para ello.

Se realizarán copias de respaldo salvo que no se hubiese producido ninguna actualización de los datos diariamente. (Si esto no fuera posible se realizará como mínimo una vez a la semana).

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

El Responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos personales, previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I, se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

Ejemplo

Las recuperaciones de datos del fichero, "fichero_ pacientes" deberán ser autorizadas por escrito por el Responsable del fichero, según el procedimiento indicado en el apartado correspondiente.

Responsable de seguridad

El Responsable del fichero designará a Miguel Gutiérrez Gutierrez, que con carácter general se encargará de coordinar y controlar las medidas definidas en este Documento de Seguridad.

En ningún caso, la designada supone una delegación de la responsabilidad que corresponde a Fernando Ruiz Ruiz como Responsable del fichero de acuerdo con el reglamento de medidas de seguridad.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de 2008. Una vez transcurrido este plazo, Fernando Ruiz Ruiz podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

En el fichero "fichero-pacientes" se conservará una copia de respaldo y de los procedimientos de recuperación de datos en el domicilio de Fernando Ruiz Ruiz, además de la que queda guardada en la propia clínica. Por ello, las copias de seguridad se realizarán siempre por duplicado.

Telecomunicaciones

La transmisión de datos de carácter personal del fichero "fichero-Datos clínicos" se realizará mediante el uso de un certificado electrónico, solicitado para la clínica a la Fábrica Nacional de Moneda y Timbre, mediante el procedimiento establecido para ello en la propia Web de dicha entidad <http://www.fnmt.es>.

En esta empresa existe un fichero manual "fichero_otras pruebas clínicas".

- El acceso a la documentación se limita exclusivamente al personal autorizado. Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados:

- Identificador. Código de registro.
- Nombre: fichero_otros datos clínicos.
- Descripción. Fichero con los datos personales de los clientes que contratan algún tipo de póliza de seguros.
  El personal autorizado sería (Fernando Ruiz Ruiz) el único autorizado para acceder a los datos.

- Los criterios de archivo se realizarán de acuerdo con la legislación que le afecte o en su defecto, los establecidos por el Responsable del fichero, que en cualquier caso garantizarán la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
- Almacenamiento de la información: Los elementos de almacenamiento como armarios o archivadores se encuentran en lugares protegidos y cuentan con llaves u otros dispositivos de seguridad. Además estos lugares permanecerán cerrados en cuanto no sea preciso el acceso a los documentos.
- Custodia de soportes: Las personas que se encuentren al cargo de la custodia de soportes deberán custodiarlos e impedir en todo momento que pueda ser accedida por personas no autorizadas.
- Traslado de documentación: Deberán adoptarse medidas orientadas a impedir el acceso o manipulación de la información objeto de traslado.
- Copias de reproducción: La realización de copias de reproducción de documentos con datos personales sólo se podrá realizar bajo el control del personal autorizado. Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida en las mismas.

C. Procedimiento general de información al personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:<indicar el procedimiento por el cual se informará a cada persona, en función de su perfil, de las normas que debe cumplir y de las consecuencias de no hacerlo. Puede ser conveniente incluir algún sistema de acuse de recibo de la información>.

<Si se estima oportuna, la remisión periódica de información sobre seguridad: circulares, recordatorios, nuevas normas, indicar aquí el procedimiento y las personas autorizadas para hacerlo>.

D. Funciones y obligaciones del personal

Funciones y obligaciones de carácter personal

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al <Responsable del fichero o de seguridad en su caso> las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento y en concreto en su Capítulo V.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones de <incluir un punto con las obligaciones detalladas de los perfiles que afectan a todos los ficheros, como, por ejemplo, administradores de los sistemas, responsables de informática, responsable/s de seguridad si existe/n, responsables de seguridad física, etc. Es importante que se concrete la persona o cargo que corresponde a cada perfil. También deben contemplarse los procedimientos de actuación o delegación de funciones para casos de ausencia. Este apartado se propone principalmente como un recopilatorio que agrupe las medidas que en el resto del documento se asignan a perfiles concretos>.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan o a los recursos del sistema de información.

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 de aquellos datos que hubiera podido conocer durante la prestación del servicio.

Se delegan las siguiente autorizaciones en los usuarios relacionados < indicar usuarios o perfiles y autorizaciones que el Responsable del fichero delega en ellos para su ejercicio>.

Caso práctico - empresa A

Funciones y obligaciones de carácter general

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal, notificar al Responsable del fichero las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones del Responsable del fichero (Pablo)

- Adoptar las medidas necesarias para que el personal usuario del Sistema de Información conozca las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en que pueden incurrir en caso de incumplimiento.
- Autorizar por escrito la ejecución de los procesos de recuperación de los datos.

- Autorizar las altas, bajas y modificaciones de los accesos de usuarios a la aplicación que realiza tratamientos de datos del fichero "fichero _clientes".
- Autorizar, en su caso, la salida de soportes informáticos con datos de carácter personal fuera de locales donde se ubica el fichero.
- Garantizar la ejecución de los derechos de acceso, modificación y supresión que ejerzan los propietarios de los datos.

Funciones y obligaciones del resto de usuarios (Juan, José y María Dolores)

- Comunicar las necesidades de administración de usuarios.
- Comunicar todas las necesidades de recuperación de datos.
- Obtener la autorización pertinente del Responsable del fichero para realizar salidas de soportes con datos de carácter personal.

Caso práctico-empresa B

Funciones y obligaciones de carácter personal

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar a Antonio Pérez Pérez o a María López López las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones del Responsable del fichero (Antonio)

- Adoptar las medidas necesarias para que el personal usuario del Sistema de Información conozca las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en que

puede incurrir en caso de incumplimiento. Esta tarea la realiza en colaboración con el responsable de seguridad.

- Autorizar por escrito la ejecución de los procesos de recuperación de datos de carácter personal, según el procedimiento de recuperación de datos.
- Autorizar las altas, bajas y modificaciones de los accesos de usuarios al Sistema de Información.
- Autorizar la salida de soportes informáticos con datos de carácter personal fuera de los locales donde se ubica el fichero.
- Adoptar las medidas correctoras pertinentes para solventar las deficiencias en materia de seguridad.
- Garantizar la ejecución de los derechos de acceso, modificación y supresión que ejerzan los propietarios de los datos.
- Incluir en los contratos de prestación de servicios, que impliquen acceso a datos de carácter personal, las cláusulas que establezcan las obligaciones de las empresas de servicios en la seguridad de los datos.

Funciones del responsable de seguridad (María)

- Notificar a la AEPD la creación, modificación y cancelación (si se produce) del fichero "fichero_clientes".
- Colaborar con el responsable del fichero, en la definición de los distintos perfiles de usuario. En dichos perfiles se especificarán las opciones de acceso permitido y el tipo de acceso requerido.
- Realizar las actividades asociadas a la gestión de administración de usuarios de la empresa. Estas se llevarán a cabo según el procedimiento y normativa de administración de usuarios.
- Concretar los datos técnicos y administrativos para llevar a cabo la administración de usuarios.
- Solicitar al responsable del fichero la preceptiva autorización cuando se produzcan salidas de soportes que contengan datos de carácter personal.
- Participar en los procesos de recuperación de datos de carácter personal.
- Validar la implantación de los requisitos de seguridad necesarios.
- Mantener actualizadas las normas y procedimientos que en materia de seguridad afecten al fichero "fichero_clientes".

- Comprobar ejecución de los controles establecidos para verificar lo dispuesto en el presente documento.
- Controlar que la auditoría se realice al menos cada dos años.
- Trasladar los informes de auditoría que periódicamente se realicen al responsable del fichero.
- Analizar los informes de auditoría y, si lo considera necesario, elevar las medidas correctoras a implantar al responsable del fichero para su aprobación.
- Confirmar la existencia en el informe de auditoría de una valoración sobre el nivel de adecuación de las medidas y controles al reglamento, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias, necesarias e incluyendo los hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
- Estar informado de los cambios que puedan producirse en las disposiciones legales sobre el tratamiento de datos de carácter personal y proponer medidas de adecuación a dichos cambios.
- Supervisar que el registro de usuarios, "usuarios.xls" se mantenga actualizado.
- Gestionar y analizar las incidencias de seguridad.
- Dictaminar medidas cuya aplicación aminoren o eliminen las incidencias acaecidas.
- Revisar periódicamente la información de control registrada sobre los accesos de los usuarios a los Sistemas de Información y elaborar mensualmente un informe de las revisiones realizadas y los problemas detectados.

Funciones y obligaciones del resto de usuarios

- Comunicar las necesidades de la administración de usuarios.
- Comunicar todas las necesidades de recuperación de datos.
- Obtener la autorización pertinente del Responsable del fichero para realizar salidas de soportes con datos de carácter personal.

Caso práctico- empresa C

Funciones y obligaciones de carácter general

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al Responsable del fichero o de seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones del Responsable del fichero (Fernando)

- Adoptar las medidas necesarias para que el personal usuario del Sistema de Información conozca las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en que puede incurrir en caso de incumplimiento. Esta tarea la realiza en colaboración con el responsable de seguridad.
- Autorizar por escrito la ejecución de los procesos de recuperación de datos de carácter personal, según el procedimiento de recuperación de datos.
- Autorizar las altas, bajas y modificaciones de los accesos de usuarios al Sistema de Información.
- Autorizar la salida de soportes informáticos con datos de carácter personal fuera de los locales donde se ubica el fichero.
- Adoptar las medidas correctoras pertinentes para solventar las deficiencias que en materia de seguridad se detecten tras la realización de las auditorías.
- Garantizar la ejecución de los derechos de acceso, modificación y supresión que ejerzan los propietarios de los datos.

Funciones del responsable de seguridad (Miguel)

- Notificar a la AEPD, la creación, modificación y cancelación (si se produce) del fichero "fichero_ Datos clínicos".
- Colaborar con el Responsable del fichero en la definición de los distintos perfiles de usuario. En dichos perfiles se especificarán las opciones de acceso permitido y el tipo de acceso requerido.
- Realizar las actividades asociadas a la gestión de administración de usuarios de la clínica. Estas se llevarán a cabo según el procedimiento y normativa de administración de usuarios.
- Concretar los datos técnicos y administrativos para llevar a cabo la administración de usuarios.
- Solicitar al Responsable del fichero la preceptiva autorización cuando se produzcan salidas de soportes que contengan datos de carácter personal.
- Participar en los procesos de recuperación de datos de carácter personal.
- Validar la implantación de los requisitos de seguridad necesarios.
- Mantener actualizadas las normas y procedimientos que en materia de seguridad afecten al fichero "fichero_Datos clínicos".
- Comprobar la ejecución de los controles establecidos para verificar lo dispuesto en el presente documento.
- Controlar que la auditoría se realice al menos cada dos años.
- Trasladar los informes de auditoría que periódicamente se realicen al Responsable del fichero.
- Analizar los informes de auditoría y, si lo considera necesario, elevar las medidas correctoras a implantar al Responsable del fichero para su aprobación.
- Confirmar la existencia, en el informe de auditoría, de una valoración sobre el nivel de adecuación de las medidas y controles al reglamento, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias e incluyendo los hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
- Estar informado de los cambios que puedan producirse en las disposiciones legales sobre el tratamiento de datos de carácter personal y proponer medidas de adecuación a dichos cambios.

- Supervisar que el registro de usuarios "usuarios.xls" se mantenga actualizado.
- Gestionar y analizar las incidencias de seguridad.
- Dictaminar medidas cuya aplicación aminoren o eliminen las incidencias acaecidas.
- Revisar periódicamente la información de control registrada sobre los accesos de los usuarios a los Sistemas de Información y elaborar mensualmente un informe de las revisiones realizadas y los problemas detectados.

Funciones y obligaciones del resto de usuarios

- Comunicar las necesidades de la administración de usuarios.
- Comunicar todas las necesidades de recuperación de datos.
- Obtener la autorización pertinente del Responsable del fichero para realizar salidas de soportes con datos de carácter personal.

E. Procedimiento de notificación, gestión y respuesta ante las incidencias

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal <denominación del Responsable del fichero>.

El procedimiento a seguir para la notificación de incidencias será <especificar concretamente los procedimientos de notificación y gestión de incidencias, indicando quién tiene que notificar la incidencia, a quién y de qué modo, así como quién gestionará la incidencia>.

El registro de incidencias se gestionará mediante <indicar la forma en que se almacenará el registro, que puede ser manual o informático, y en el que deberán constar, al menos, 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 comunica y los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas. En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

A

NIVEL MEDIO

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros <relacionar los ficheros de nivel medio y alto>, del modo que se indica a continuación <detallar el procedimiento para registrar las recuperaciones de datos que deberá incluir 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. En caso de gestión automatizada, se deberá prever la existencia de un código específico para recuperaciones de datos, en la información relativa al tipo de incidencia>.

NIVEL MEDIO

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior será necesaria la autorización por escrito del Responsable del fichero.

En el Anexo III se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

Caso práctico - empresa A

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del fichero controlado por Pablo García García.

El procedimiento a seguir para la notificación de incidencias será: la incidencia será anotada por quien la detecte y enviada al Responsable del fichero. Este anotará en el registro de incidencias, haciendo constar el tipo de incidencia y el momento en que se ha producido, la persona que realiza la notificación y los efectos que se hubieran derivado de la misma. Posteriormente, el Responsable del fichero se encargará de tomar las medidas oportunas.

El registro de incidencias se gestionará mediante un documento Word llamado "incidencias.doc", en el que se anotarán los datos relativos a cada incidencia, (tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma). Este documento es editado utilizando Microsoft Office 2007.

En el Anexo III se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimiento de recuperación de datos.

Caso práctico - empresa B

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del fichero controlado por Antonio Pérez Pérez.

La incidencia será anotada por quien la detecte y enviada al Responsable del fichero (Antonio). Este la anotará en el registro de incidencias haciendo constar el número de incidencia (exclusivo para cada una), tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación y los efectos que hubieran derivado de la misma. Posteriormente, el Responsable del fichero se encargará de tomar las medidas oportunas.

El registro de incidencias se gestionará mediante un documento Excel llamado "incidencias.xls", en el que se anotarán los campos relativos a cada incidencia (tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma). Este documento es editado utilizando Microsoft Office 2007.

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten al fichero "fichero _clientes", del modo que se indica a continuación. El Responsable del fichero autorizará a la persona que se encargará de realizar la recuperación de datos. Por defecto y si no lo impide una causa de fuerza mayor, la persona encargada de realizar la recuperación de datos será María López López. Dicha persona se encargará de acceder al soporte que contenga los datos a recuperar y ejecutar las acciones

necesarias para restaurarlos. Una vez concluido el proceso, se realizará el correspondiente registro en el fichero de incidencias, anotando el número de la incidencia, nombre del que restaura, la fecha, la hora y qué tipo de datos se han recuperado.

Ejemplo

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior será necesaria la autorización por escrito del Responsable del fichero.

Ejemplo

En los ficheros manuales, en este caso "fichero _documentación de los clientes", aplicaremos el mismo procedimiento de notificación, gestión y respuesta ante las incidencias que en los ficheros automatizados.

En el Anexo III se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimientos de recuperación de dato.

Caso práctico - empresa C

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del fichero controlado por Fernando Ruiz Ruiz.

La incidencia será anotada por quien la detecte y enviada al Responsable del fichero (Fernando). Este la anotará en el registro de incidencias haciendo constar el número de incidencia (exclusivo para cada una), tipo de incidencia, en el momento en que se ha producido, la persona que realiza la notificación y los efectos que hubieran derivado de la misma. Posteriormente, el Responsable del fichero se encargará de tomar las medidas oportunas.

El registro de incidencias se gestionará mediante un documento llamado "incidencias, ods", en el que se anotarán los campos relativos a cada incidencia (tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma). Este documento es editado utilizando Open Office.org 2.0.

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten al fichero "fichero_ pacientes", del modo que se indica a continuación.

Ejemplo

El Responsable del fichero autorizará a la persona que se encargará de realizar la recuperación de datos, que será Miguel Gutiérrez.

Dicha persona (Miguel Gutiérrez) se encargará de acceder al soporte que contenga los datos a recuperar y ejecutar las acciones necesarias para restaurarlos. Una vez concluido el proceso se realizará el correspondiente registro en el fichero de incidencias, anotando el número de la incidencia, nombre del que restaura, la fecha, la hora y qué tipo de datos se han recuperado.

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del Responsable del fichero.

En el Anexo III se incluirán los documentos de autorización por parte del Responsable del fichero relativos a la ejecución de procedimientos de datos.

Ejemplo

En los ficheros manuales, al igual que hemos visto en el caso anterior, se aplicará el mismo procedimiento de notificación, gestión y respuestas ante las incidencias que en los ficheros automatizados, el fichero manual que tenemos en el caso C es "fichero_otras pruebas clínicas".

F. Procedimientos de revisión

<Especificar los procedimientos previstos para la modificación del Documento de Seguridad, con especificación concreta de las personas que pueden o deben proponerlos y aprobarlos, así como para la comunicación de las modificaciones al personal que pueda verse afectado.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso, se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal>.

NIVEL MEDIO. AUDITORÍA

<Indicar los procedimientos para realizar la auditoría interna o externa que verifique el cumplimiento del Título VIII del RLOPD, referente a las medidas de seguridad, según lo indicado en sus artículos 96 y 110 respecto de ficheros

automatizados y no automatizados respectivamente, y que debe realizarse al menos cada dos años.

A

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan 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 dos años señalado.

El informe analizará la adecuación de las medidas y controles a la ley y su desarrollo reglamentario identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente que elevará las conclusiones al Responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos o en su caso de las autoridades de control de las Comunidades Autónomas>.

NIVEL ALTO. INFORME MENSUAL SOBRE EL REGISTRO DE ACCESOS

<Indicar los procedimientos para realizar el informe mensual sobre el registro de accesos a los datos de nivel alto regulado por el artículo 24 del RLOPD>.

Caso práctico- empresa A

Actualizar el Documento de Seguridad

El Documento de Seguridad permanece archivado en el Sistema de Información de la empresa como documento Word, siendo Pablo el único que tiene acceso al mismo. Ante los siguientes supuestos:

- Cambios en la organización de seguridad.
- Cambios en las normativas o procedimientos del Documento de Seguridad.

- Cambios importantes en los Sistemas de Información.
- Cambios efectuados para adecuarse a las disposiciones legales en materia de seguridad de datos de carácter personal.

El Responsable del fichero (Pablo) estudiará y, en su caso, efectuará la modificación con los cambios necesarios. Una vez realizadas las modificaciones con los cambios necesarios, se encargará de la emisión y difusión de la nueva versión del documento.

Caso práctico- empresa B

Actualizar el Documento de Seguridad

El Documento de Seguridad permanece archivado en el sistema como documento Word, siendo el responsable de seguridad y el Responsable del fichero los únicos que tienen acceso al mismo. Ante los siguientes supuestos:

- Cambios en la organización de seguridad.
- Cambios en las normativas o procedimientos del Documento de Seguridad.
- Cambios importantes en los Sistemas de Información.
- Cambios efectuados para adecuarse a las disposiciones legales en materia de seguridad de datos de carácter personal.

La responsable de seguridad (María) revisará el presente documento y elaborará una propuesta de modificación que presentará al Responsable del fichero. El Responsable del fichero (Antonio) estudiará la propuesta de modificación y, en su caso, autorizará la modificación con los cambios que él mismo acuerde. Una vez aprobada la propuesta de modificación del presente documento, la responsable de seguridad realizará las modificaciones oportunas en el mismo. La responsable de seguridad se encargará de la emisión y difusión de la nueva versión del documento.

Auditoría

Cada dos años será llevada a cabo una auditoría de seguridad que verifique el nivel de cumplimiento del RLOPD (RD 1720/2007, de 21 de diciembre) en la empresa. Esta auditoría será interna y el responsable de llevarla a cabo será el empleado Pedro Jiménez Jiménez. El informe de dicha auditoría será enviado al Responsable del fichero (Antonio), que lo analizará y tomará las medidas oportunas. Este informe quedará archivado por si fuera requerido en cualquier momento por la Agencia Española de Protección de Datos.

Caso práctico-empresa C

Actualizar el Documento de Seguridad

El Documento de Seguridad permanece archivado en el Sistema de Información de la clínica, como documento de OpenOffice. Org Writer, siendo Fernando y Miguel (el responsable de seguridad) los únicos que tienen acceso al mismo. Ante los siguientes supuestos:

- Cambios en la organización de seguridad.
- Cambios en las normativas o procedimientos del Documento de Seguridad.
- Cambios importantes en los Sistemas de Información.
- Cambios efectuados para adecuarse a las disposiciones legales en materia de seguridad de datos de carácter personal.

El Responsable del fichero (Miguel) revisará el presente documento y elaborará una propuesta de modificación que presentará al Responsable del fichero (Fernando). El Responsable del fichero estudiará la propuesta de modificación y, en su caso, autorizará la modificación con los cambios que él mismo acuerde. Una vez aprobada la propuesta de modificación del presente documento, el responsable de seguridad realizará las modificaciones oportunas en el mismo. El propio responsable de seguridad se encargará de la emisión y difusión de la nueva versión del documento.

Auditoría

Cada dos años será llevada a cabo una auditoría que verifique el nivel de cumplimiento del RLOPD (Real Decreto 1720/2007, de 21 de diciembre) en la empresa. Esta auditoría será interna y la responsable de llevarla a cabo será Teresa Muñoz Muñoz. El informe de dicha auditoría será enviado al Responsable del fichero (Fernando) que lo analizará y tomará las medidas oportunas. Este informe quedará archivado por si fuera requerido en cualquier momento por la Agencia Española de Protección de Datos.

Ejemplo

Informe mensual sobre el "Registro de Accesos". El registro de accesos será analizado por el responsable de seguridad (Miguel) una vez al mes. Tras su análisis escribirá un informe que enviará al Responsable del fichero. Este informe se realizará conforme a los procedimientos regulados en el artículo 24 RLOPD.

G. Consecuencias del incumplimiento del documento de seguridad

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a <indicar la normativa sancionadora aplicable>.

ANEXO I. DESCRIPCIÓN DE FICHEROS

A. ASPECTOS RELATIVOS AL FICHERO...

Actualizado a. <Fecha de la última actualización del anexo>.

<Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del Documento de Seguridad, podrían denominarse Anexo I a, b, c, etc.>.

- Nombre del fichero o tratamiento.<Rellenar con nombre del fichero>.
- Unidad/es con acceso al fichero o tratamiento. <Especificar departamento o unidad con acceso al fichero, si aporta alguna información>.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos. <Rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>.

    - Identificador. <Código de inscripción>.
    - Nombre. <Nombre inscrito>.
    - Descripción. <Descripción inscrita>.

- Nivel de medidas de seguridad adoptar. <Básico, medio o alto>.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

<Persona designada por el Responsable del Fichero al objeto de coordinar y controlar las medidas incluidas en este documento para este fichero, en el caso de que existan varios o para todos los ficheros en el supuesto de que se trate de designación única>.

- Administrador. <Persona designada para conceder, alterar o anular el acceso autorizado a los datos>.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>.
- Código Tipo Aplicable. <Se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal. <Incorporar los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 81 del Reglamento de desarrollo de la LOPD>.
- Información sobre el fichero o tratamiento:

- Finalidad y usos previstos.
- Personas o colectivos sobre los que se pretenda obtener o que estén obligados a suministrar los datos personales.
- Cesiones previstas.
- Transferencias Internacionales. <Relacionar las transferencias internacionales especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>.
- Procedencia de los datos. <Indicar quién suministra los datos>.
- Procedimiento de recogida. <Encuestas, formularios en papel, Internet,...>.
- Sistema de tratamiento. <Automatizado, manual o mixto>.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición. <Indicar la unidad y/o dirección. Deben preverse además los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación. <Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.
- Información sobre conexión con otros sistemas. <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales. <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación. <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado. <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.
- <Si la relación se mantiene de forma informatizada indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este anexo>.

- Terceros que acceden a los datos para la prestación de un servicio: <relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.
- Relación de actualizaciones de este anexo. <Incluyendo fecha, resumen de aspectos modificados y motivo>.

B. ASPECTOS RELATIVOS AL FICHERO...

ANEXO II. NOMBRAMIENTOS

<Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad>.

ANEXO III. AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

<Adjuntar original o copia de las autorizaciones que el Responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos>.

ANEXO IV. INVENTARIO DE SOPORTES

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el Capítulo II, punto "Gestión de soportes" de este documento. Los soportes 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 este documento>.

ANEXO V. REGISTRO DE INCIDENCIAS

<Si el registro de incidencias se gestiona de forma actualizada, recoger en este anexo la información al efecto, según lo indicado en el capítulo V "Procedimiento de notificación, gestión y respuesta ante las incidencias" de este documento>.

ANEXO VI. ENCARGADO DE TRATAMIENTO

<Cuando el acceso de un tercero a los datos del Responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido y que establecerá expresamente que el Encargado del tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará ni si quiera para su conservación a otras personas>.

<El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD, que el Encargado del tratamiento está obligado a implementar>.

ANEXO VIII. REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el Capítulo II, punto "Gestión de soportes" y que es obligatorio a partir del nivel medio, se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado en el artículo 97 del Reglamento de desarrollo de la LOPD>.

Caso práctico-empresa A

ANEXO I. Aspectos relativos al fichero "fichero_ clientes"

Actualizado a: 20-03-2008

- Nombre del fichero o tratamiento: fichero_clientes.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:
  - Identificador. El asignado por la AEPD.
  - Nombre: fichero_clientes.
  - Descripción. Fichero con los datos personales de los clientes de la empresa.

- Nivel de medidas de seguridad a adoptar. Básico.
- Administrador. Pablo García García.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento. LOPD y Real Decreto 1720/2007.
- Código Tipo Aplicable. Ninguno.
- Estructura del fichero principal. Nombre del cliente, DNI, domicilio, teléfono fijo, teléfono móvil, fecha de nacimiento, tarjeta/contrato tipo.
- Información sobre el fichero o tratamiento:

    - Finalidad y usos previstos: Gestionar los gastos e ingresos de la empresa, así como enviar publicidad e información de productos mediante correo ordinario.
    - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales. Los clientes que adquieran algún producto en la tienda.
    - Cesiones previstas. Ninguna.
    - Transferencias Internacionales. Ninguna.
    - Procedencia de datos. Del propio cliente.
    - Procedimiento de recogida de datos. El cliente entrega su DNI al dependiente.
    - Soporte utilizado para la recogida de datos. Informático.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición. LOPD COMUNICACIONES S.L., c/Fresca nº 147- Antequera (Málaga). Cualquier cliente puede acceder a sus datos mediante la entrega del DNI al dependiente.
- Descripción del sistema de información: El sistema de información se encuentra implantado en tres ordenadores personales, todos ellos con procesador Athlon XP 3000+, 1Gbyte de memoria DDR y disco duro de 40 Gbytes. Se utiliza Sistema Operativo Windows 2000 Profesional. El Sistema Gestor de Bases de Datos utilizado es ORACLE 8.0 y la aplicación que actúa de interface con la base de datos está implementada en Delphi 5. Los ordenadores se encuentran conectados mediante red Fast Ethernet.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación:

1. Obtener copias de respaldo:

   - Finalizada la jornada laboral y cuando los sistemas de información no estén operativos se ejecutan los procesos de copias de respaldo, los cuales están previamente programados de forma diaria.
   - La persona encargada (José) selecciona, en su caso, los soportes a utilizar de acuerdo con el sistema de rotación establecido y procede a realizar las copias de respaldo.
   - Una vez obtenidas las copias de respaldo, se actualizará el registro de soportes.
   - Finalmente, la persona encargada (José) etiqueta y almacena los soportes que contienen las copias de respaldo en el armario cerrado con llave por orden de fechas.

2. Recuperación de datos:

   - Ante una necesidad de recuperación de datos, el usuario lo comunica al Responsable del fichero.
   - El Responsable del fichero (Pablo) analiza la necesidad de recuperación y decide, si es preciso, qué ficheros y datos se recuperan, en qué momento, a partir de qué copias de respaldo y si es necesario grabar datos manualmente.
   - El Responsable del fichero autoriza por escrito la ejecución de los procesos de recuperación de ficheros.
   - El Responsable del fichero entrega al usuario designado por él una solicitud formal de ejecución del proceso de recuperación de los datos.
   - El usuario designado (José) recupera físicamente los datos a partir de los ficheros requeridos.
   - Una vez recuperados los datos, el Responsable del fichero (Pablo) registra las acciones asociadas a la incidencia y cierra esta.

- Información sobre conexión con otros sistemas. No las hay.
- Funciones del personal con acceso a los datos personales:

  - Responsable del fichero (Pablo García García). Autorizar la creación y estructura del fichero de datos, autorizar su modificación y eliminación. Dar autorizaciones que se establecen en este documento.

Utilizar el fichero de clientes para gestionar los gastos e ingresos. Velar por el cumplimiento de las medidas de seguridad recogidas en este documento. Actualizar el presente documento.

- Funciones del resto de usuarios (Juan, José y María Dolores). Recoger y tratar los datos de los clientes cumpliendo las normas y procedimientos recogidos en este documento. Notificar cualquier incidencia de seguridad al Responsable del fichero. Además, de forma normal y si otra circunstancia no lo impide, José será el encargado de llevar a cabo los procesos de copia y recuperación de datos.

- Descripción de los procedimientos de control de acceso e identificación: Cada usuario entrará al sistema mediante la introducción de su nombre de usuario y su contraseña.
- Relación actualizada de usuarios con acceso autorizado: La relación de usuarios se encuentra escrita en documento Word, llamado "usuarios.doc" dentro del Sistema de Información de la empresa. Para imprimirlo sólo hay que abrirlo con la aplicación MS Word 2000 y pulsar el botón "Imprimir".
- Terceros que acceden a los datos para la prestación de un servicio. No los hay.

Relación de actualizaciones de este anexo. Ninguna actualización desde la fecha de creación.

NOMBRE	GRUPO	CORREO ELECTRÓNICO	FECHA DE ALTA	FECHA DE BAJA
Pablo García García	Administradores	pablo@lopdcom	20-01-2007	20-01-2008
Juan López López	Dependientes	uan@lopdcom	20-01-2007	20-01-2008
José Pérez García	Dependientes	jose@lopdcom	20-01-2007	20-01-2008
Mª Dolores Jiménez Ruíz	Dependientes	mdores@lopdcom	20-01-2007	20-01-2008

ANEXO II Nombramientos

Pablo García García. Responsable del fichero y administrador del sistema.

José Pérez García. Encargado de llevar a cabo los procesos de copia y recuperación de datos.

ANEXOS III Autorizaciones salida o recuperación de datos

Ninguna hasta la fecha.

ANEXOS IV Inventario de soportes

Ninguno hasta la fecha, porque no hay ningún fichero no automatizado.

ANEXOS V: Registro de incidencias

Ninguno hasta la fecha.

ANEXOS VI: Encargado de tratamiento

Cuando el acceso de un tercero a los datos del Responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos.

ANEXOS VII: Registro de entrada y salida de soportes

No existe.

Caso práctico-empresa B

ANEXO I. Aspectos relativos al fichero "fichero_clientes"

Actualizado a: 21-03-08.

- Nombre del fichero o tratamiento: "fichero_clientes".

- Unidad/es con acceso al fichero o tratamiento. El administrador (Antonio Pérez Pérez), la responsable de seguridad (María López López) y el empleado Pedro Jiménez Jiménez.
- Identificador y nombre del fichero, en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:

  - Identificador. Código de registro.
  - Nombre: fichero_ clientes.
  - Descripción. Fichero con los datos personales de los clientes que contratan algún tipo de póliza de seguros.

- Nivel de medidas de seguridad a adoptar. Medio.
  Responsable de seguridad. María López López.
- Administrador. Antonio Pérez Pérez.
- Leyes o regulaciones aplicables, que afectan al fichero o tratamiento. LOPD y Real Decreto 1720/2007.
- Código Tipo Aplicable. Ninguno.
- Estructura del fichero principal:

  - Nº DE PÓLIZA, FECHA DE VENCIMIENTO, DNI DEL TOMADOR, NOMBRE DEL TOMADOR, DOMICILIO, TIPO DE SEGURO, BENEFICIARIO E IMPORTE DE LA PRIMA.

- Información sobre el fichero o tratamiento:

  - Finalidad y usos previstos. Gestión de clientes, gestión de pagos y cobros.
  - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales. Los clientes que contraten cualquier tipo de póliza de seguros.
  - Cesiones previstas. Ninguna.
  - Transferencias Internacionales. No se prevén.
  - Procedencia de los datos. Los propios clientes.
  - Procedimientos de recogida. El cliente rellenará un formulario de solicitud de póliza que contendrá sus datos personales. Este formu-

lario se entregará al dependiente para ser registrado en la base de datos del sistema.

- Soporte utilizado para la recogida de datos. Impreso de solicitud que se cumplimentará a mano para posteriormente introducir los datos en soporte informático.

- Servicio o Unidad, ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición. LOPD SEGUROS S.L c/Carreteros nº 123- Antequera (Málaga).
- Descripción del sistema de información. El sistema consta de cuatro ordenadores personales conectados en red Fast Ethernet. Todos los ordenadores tienen instalado Sistema Operativo Windows XP Home Edition. El ordenador de Antonio actúa como servidor de la base de datos soportada por el sistema Paradox y los demás acceden a dicha base de datos, mediante la aplicación interface escrita en Delphi. Todos los ordenadores tienen instalado el paquete ofimático MS Office 2000.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación. Las copias de respaldo se realizarán diariamente de forma incremental, excepto cuando no se produzca ninguna modificación del fichero durante ese periodo de tiempo. El proceso de copia y recuperación de datos es el siguiente:

1. Obtener copias de respaldo.

   - Finalizada la jornada laboral y cuando los sistemas de información no estén operativos se ejecutan los procesos de copias de respaldo, los cuales están previamente programados de forma diaria.
   - La persona encargada (Pedro) selecciona en su caso los soportes a utilizar de acuerdo con el sistema de rotación establecido y procede a realizar las copias de respaldo.
   - Una vez obtenidas las copias de respaldo se actualizará el registro de soportes.
   - Finalmente, la persona encargada (Pedro) etiqueta y almacena los soportes que contienen las copias de respaldo en el armario cerrado con llave por orden de fechas.

2. Recuperación de datos.

- Ante una necesidad de recuperación de datos, el usuario lo comunica al responsable de seguridad (María).
- La Responsable de seguridad (María) analiza la necesidad de recuperación y decide, si es preciso, qué ficheros y datos se recuperan, en qué momento, a partir de qué copias de respaldo y si es necesario grabar datos manualmente.
- El Responsable del fichero (Antonio) autoriza por escrito la ejecución de los procesos de recuperación de ficheros.
- La responsable de seguridad (María) entrega a Pedro una solicitud formal de ejecución del proceso de recuperación de los datos.
- Pedro recupera físicamente los datos a partir de los ficheros requeridos.
- Una vez recuperados los datos, la responsable de seguridad registra las acciones asociadas a la incidencia y cierra esta.

- Información sobre conexión con otros sistemas. No se da el caso.
- Funciones del personal con acceso a los datos personales:

- Responsable del fichero (Antonio Pérez Pérez):
  Autorizar la creación y estructura del fichero de datos, autorizar su modificación y eliminación. Dar las autorizaciones que se establecen en este documento.
  Utilizar el fichero de clientes para gestionar los gastos e ingresos.
  Velar por el cumplimiento de las medidas de seguridad recogidas en este documento. Tomar las decisiones oportunas a partir del informe de auditoría. Actualizar el presente documento.
- Responsable de seguridad (María López López). Con carácter general, se encargará de coordinar y controlar las medidas definidas en este Documento de Seguridad.
- Funciones del resto de usuarios (Pedro Jiménez Jiménez). Recoger y tratar los datos de los clientes, cumpliendo las normas y procedimientos recogidos en este documento. Notificar cualquier incidencia de seguridad al Responsable del fichero.

- Descripción de los procedimientos de control de acceso e identificación: Los ya descritos con anterioridad en este documento, en el apartado de Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales y en el apartado "Control de acceso".
- Relación actualizada de usuarios con acceso autorizado:

NOMBRE	GRUPO	CORREO ELECTRÓNICO	FECHA DE ALTA	FECHA DE BAJA
Antonio Pérez Pérez	Administradores	antonio@lopdsegur	12-01-2007	12-01-2008
María López López	Seguridad	maria@lopsdsegur	12-01-2007	12-01-2008
Pedro Jímenez	Gestores	pedro@lopdsegur	12-01-2007	12-01-2008

Esta relación de usuarios se encuentra escrita en un documento de Excel llamado "usuarios.xls", al que sólo el Responsable del fichero y el responsable de seguridad tienen acceso para su modificación. El fichero puede editarse con la aplicación ofimática MS Excel 2000. Para su impresión sólo hay que pulsar el botón "imprimir".

- Terceros que acceden a los datos para la prestación de un servicio: No los hay.
- Relación de actualizaciones de este anexo. Sin actualizaciones hasta el momento.

ANEXO II Nombramientos

Antonio Pérez Pérez. Responsable del fichero.

María López López. Responsable de seguridad.

Pedro Jiménez Jiménez. Responsable de realizar la auditoría interna y los procesos de copia y recuperación de datos.

ANEXO III Autorizaciones salida o recuperación de datos

Ninguna hasta el momento.

ANEXO IV Inventario de soportes

Si el inventario de soportes se gestiona de forma no automatizada, los soportes 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 este documento.

ANEXO V Registro de incidencias

Ninguno hasta el momento.

ANEXO VI Encargado de tratamiento

En este caso el acceso al fichero o tratamiento lo tiene el administrador (Antonio Pérez Pérez), la responsable de seguridad (María López López) y el empleado (Pedro Jiménez Jiménez).

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD, que el encargado del fichero está obligado a implementar.

ANEXO VII Registro de entrada y salida de soportes

Ninguno hasta el momento.

En los ficheros no automatizados se sigue el mismo procedimiento que para los ficheros automatizados.

Caso práctico-empresa C

ANEXO I. Aspectos relativos al fichero "fichero_ pacientes"

Actualizado a: 16-03-2011.

- Nombre del fichero o tratamiento: "fichero_ Datos clínicos".
- Unidad/ es con acceso al fichero o tratamiento. El administrador (Fernando Ruiz Ruiz), el responsable de seguridad (Miguel Gutiérrez Gutiérrez) y las encargadas del tratamiento (Teresa Muñoz Muñoz, Marta Luque Luque y Sonia Martín Martín).
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos:

  - Identificador. Código de registro dado por la AEPD.
  - Nombre: fichero_ Datos clínicos.
  - Descripción. Fichero con los datos personales de los pacientes de la clínica.

- Nivel de medidas de seguridad a adoptar. Nivel alto.
  Responsable de seguridad. Miguel Gutiérrez Gutiérrez.
- Administrador. Fernando Ruiz Ruiz.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento. LOPD Y Real Decreto 1720/2007.
- Código Tipo Aplicable. Ninguno.
- Estructura del fichero principal:

Tabla: Ficha pacientes

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

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

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

- Información sobre el fichero o tratamiento:
  - Finalidad y usos previstos. Gestión de pacientes, gestión de contabilidad.
  - Personas o colectivos sobre los que se pretende obtener o que resulten obligados a suministrar los datos personales. Los pacientes que soliciten los servicios de la clínica.
  - Cesiones previstas. Ninguna.

- Transferencias Internacionales. No se prevén.
- Procedencia de los datos. Los propios pacientes.
- Procedimiento de recogida. Mediante entrevista.
- Soporte utilizado para la recogida de datos. Los datos de carácter personal quedarán recogidos en soporte informático. Las pruebas de diagnóstico (radiografías, etc.) quedarán recogidas en soporte manual.

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición. LOPD-ODONTOS S.L c/Carreteros nº 124 - Antequera (Málaga).
- Descripción del sistema de información. La clínica dispone de tres ordenadores personales conectados a Internet, todos ellos con un procesador Pentium 4.512 Mbyte de memoria principal y disco duro de 80 Gbytes. El Sistema operativo instalado es Guadalinex 2004, el cual incluye entre otras aplicaciones el paquete ofimático OpenOffice.org 2.0. El sistema gestor de bases de datos utilizado es MySQL 5. Los datos son accedidos mediante una aplicación visual escrita en lenguaje Python.
  Los ordenadores están conectados en red inalámbrica 802.11 g mediante un Router wireless, que los conecta entre sí y les posibilita conexión a Internet.
- Descripción detallada de las copias respaldo y de los procedimientos de recuperación. Las copias de respaldo se realizarán diariamente de forma incremental, excepto cuando no se produzca ninguna modificación del fichero durante este periodo de tiempo. El proceso de copia y recuperación de datos es el siguiente:

  1. Obtener copias de respaldo.

     - Finalizada la jornada laboral y cuando los sistemas de información no estén operativos se ejecutan los procesos de copias de respaldo, los cuales están previamente programados de forma diaria.
     - La persona encargada (Pedro) selecciona, en su caso, los soportes a utilizar de acuerdo con el sistema de rotación establecido y procede a realizar las copias de respaldo.
     - Una vez obtenidas las copias de respaldo se actualizará el registro de soportes.

- Finalmente, la persona encargada (Pedro) etiqueta y almacena los soportes que contienen las copias de respaldo en el armario cerrado con llave por orden de fechas.

2. Recuperación de datos.

- Ante una necesidad de recuperación de datos, el usuario lo comunica al responsable de seguridad (María).
- La responsable de seguridad (María) analiza la necesidad de recuperación y decide, si es preciso, qué ficheros y datos se recuperan, en qué momento, a partir de qué copias de respaldo y si es necesario grabar datos manualmente.
- El Responsable del fichero (Antonio) autoriza por escrito la ejecución de los procesos de recuperación de ficheros.
- La responsable de seguridad (María) entrega a Pedro una solicitud formal de ejecución del proceso de recuperación de los datos.
- Pedro recupera físicamente los datos a partir de los ficheros requeridos.
- Una vez recuperados los datos, la responsable de seguridad registra las acciones asociadas a la incidencia y cierra esta.

- Información sobre conexión con otros sistemas. No se da el caso.
- Funciones del personal con acceso a los datos personales:

  - Fernando Ruiz Ruiz (administrador). Autorizar la creación y estructura de los ficheros con datos de carácter personal. Autorizar la entrada y salida de soportes. Realizar las anotaciones correspondientes en el registro de entrada y salida de soportes. Será quién se encargue de dar de alta, modificar o dar de baja las autorizaciones de acceso a los datos.
  - Miguel Gutiérrez Gutiérrez (responsable de seguridad). Con carácter general, se encargará de coordinar y controlar las medidas definidas en este Documento de Seguridad. También podrá ejercer las funciones de cualquier otro usuario, excepto las de Fernando Ruiz Ruiz.
  - Teresa Muñoz Muñoz (usuario avanzado). Guardar las medidas de seguridad establecidas en este documento a la hora de recoger y

tratar datos de carácter personal o los relativos a la salud de los clientes recogidos en las tres tablas del fichero de la base de datos, así como notificar cualquier incidencia que se produzca en lo referente a la seguridad de los datos personales.

- Sonia Martín Martín (usuario normal). Guardar las medidas de seguridad establecidas en este documento a la hora de recoger y tratar los datos personales de los pacientes recogidos en la tabla "Pacientes" del fichero de la base de datos, así como notificar cualquier incidencia que se produzca en lo referente a la seguridad de los datos personales. También llevará a cabo los procesos de copia y recuperación de datos.
- Marta Luque Luque (usuario normal). Guardar las medidas de seguridad establecidas en este documento a la hora de recoger y tratar los datos personales de los pacientes recogidos en la Tabla "Pacientes" del fichero de la base de datos, así como notificar cualquier incidencia que se produzca en lo referente a la seguridad de los datos personales.

- Descripción de los procedimientos de control de acceso e identificación:

  - El Responsable del fichero (Fernando) será quien se encargue de dar de alta, modificar o dar de baja las autorizaciones de acceso a los datos mediante la incorporación de nuevos usuarios en el sistema y su asignación o modificación de un perfil de usuario. Todos los usuarios que se crean tienen como contraseña predeterminada la asignada por Fernando, que se la entregará por escrito al nuevo usuario para su consulta privada y personal.
  - Cada vez que un usuario entra en el sistema se modifica un archivo "log" que almacena cada uno de los accesos que el usuario realiza al fichero de pacientes, con indicación del dato concreto al que accede y la operación que realiza sobre el mismo. Este fichero sólo es accesible por el usuario administrador (en este caso Fernando) y por el responsable de seguridad (Miguel).

- Relación actualizada de usuarios con acceso autorizado. Esta relación de usuarios se encuentra escrita en un documento llamado "usuarios.ods"

al que sólo el Responsable del fichero tiene acceso para su modificación. El fichero puede editarse con la aplicación ofimática OpenOffice.org Calc. Para su impresión sólo hay que pulsar en el botón "imprimir".

- Terceros que acceden a los datos para la prestación de un servicio. No los hay.
- Relación de actualizaciones de este anexo. Sin actualizaciones hasta el momento.

ANEXO II Nombramientos

Fernando Ruiz Ruiz. Responsable del fichero.

Miguel Gutiérrez Gutiérrez . Responsable de seguridad.

Sonia Martín Martín. Responsable de llevar a cabo los procesos de copia y recuperación de datos.

ANEXO III Autorizaciones salida o recuperación de datos

Ninguna hasta la fecha.

ANEXO IV Inventario de soportes

El soporte utilizado para la recogida de datos en este caso son:

Los de carácter personal quedarán recogidos en soporte informático.

Las pruebas de diagnóstico (radiografías, etc.) quedarán recogidas en soporte manual.

ANEXO V Registro de incidencias

Ninguno hasta la fecha.

ANEXO VI Encargado del tratamiento

Cuando el acceso de un tercero a los datos del Responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos.

ANEXO VII. Registro de entrada y salida de soportes

Ninguna hasta la fecha.

En los ficheros no automatizados se sigue el mismo procedimiento que en los ficheros no automatizados.