DOCUMENTO DE SEGURIDAD

RELATIVO AL FICHERO MIXTO

Página web/ Correo electrónico

CON DATOS DE CARÁCTER PERSONAL

Y NIVEL DE SEGURIDAD BÁSICO INCLUIDO

EN EL RGPD CON EL NÚMERO:

2141501382

Responsable	**RÓTULOS RODRÍGUEZ S.L.**
Fecha de edición	**29 de Mayo de 2014**

OBJETO DEL DOCUMENTO

El Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por R.D. 1720/2007, de 21 de diciembre, en su artículo 88 establece que el responsable del fichero elaborará un documento que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimento para el personal con acceso a datos de carácter personal.

Este documento de seguridad recopila las normas y los procedimientos necesarios para aplicar estas medidas de seguridad, de obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas e instalaciones que los soportan, y que deben servir para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal.

Este documento deberá mantenerse permanentemente 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.

El fichero de datos **Página web/ Correo electrónico**, descrito en el documento resumen de la notificación a la Agencia Española de Protección de Datos (AEPD) adjunto en el Anexo A y detallado estructuralmente en el Anexo B, se encuentra oficialmente clasificado con nivel de seguridad básico, atendiendo a las condiciones descritas en el artículo 81 del R.D. 1720/2007, siendo por tanto aplicable a él todas las medidas de seguridad de nivel básico que se establecen en el Capítulo III del Título VIII del citado Real Decreto.

ÁMBITO DE APLICACIÓN

El alcance para la aplicación de las medidas de seguridad, que se definen en el presente documento de seguridad, es para todos aquellos recursos que, tal y como establece el Reglamento tienen que ser objeto de protección, al formar parte de los sistemas, recursos o soportes de los datos de carácter personal relativos a los sistemas de información.

El presente Documento será de aplicación al fichero, sea automatizado o no automatizado (documento), que contiene datos de carácter personal y que se halla bajo la responsabilidad del responsable del fichero, 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. La mención al término “fichero” comprenderá cualquiera de los dos tipos contemplados en el presente párrafo; cuando se pretenda una referencia concreta a uno u otro tipo, se hará constar debidamente.

Todas las personas que tengan acceso a los datos del fichero, bien a través de una aplicación informática específicamente diseñada para acceder a los mismos, bien a través de cualquier otro medio de acceso a los ficheros (otras herramientas informáticas, Internet, etc.), o bien de forma presencial en el caso de ficheros no automatizados o documentos, se encuentran obligadas por ley a cumplir lo establecido en este documento y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte, será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

RECURSOS PROTEGIDOS

La protección de los datos del fichero frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.
Los recursos que, por servir de medio directo o indirecto para acceder al fichero, deberán ser controlados por esta normativa son:

1. Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan. (Anexo C)
2. Los equipos, bien locales o remotos, desde los que se puede tener acceso al fichero. (Anexo D)
3. Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el fichero. (Anexo E)
4. Las aplicaciones establecidas para acceder a los datos. (Anexo F)

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Este documento de seguridad es de obligado cumplimiento para todas las figuras que se describen a continuación:

RESPONSABLE DEL FICHERO

- Función

El responsable del fichero es la persona física o jurídica que tiene la responsabilidad de definir las medidas de seguridad establecidas en el presente documento.

Además, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

El responsable del fichero se encargará de la difusión del documento de seguridad, coordinará la puesta en marcha de las medidas de seguridad y se encargará del control del cumplimiento de las mismas.

- Obligaciones

El responsable del fichero implantará las medidas de seguridad establecidas en este documento y garantizará la difusión del mismo entre todo el personal que lo vaya a utilizar.

Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en el fichero o tratamiento o, en su caso, como consecuencia de los controles periódicos realizados; asimismo, deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.

Entorno de sistema operativo y de comunicaciones.
Aprobará o designará al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo G.

Sistema informático o aplicaciones de acceso al fichero.
El responsable del fichero se encargará de que los sistemas informáticos de acceso al fichero tengan su acceso restringido mediante un código de usuario y una contraseña.

Asimismo cuidará que todos los usuarios autorizados para acceder al fichero, relacionados en el Anexo G, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

El responsable del fichero asignará de forma personalizada a cada usuario del sistema de información con acceso al fichero y, en su caso, a cada usuario con acceso a documentos que contengan datos de carácter personal, las funciones y responsabilidades en relación con la confidencialidad y protección de los datos que, por su puesto de trabajo, ha de procesar, manipular o custodiar, dejando constancia escrita de su "enterado" o "recibí" en el presente documento (Anexo H).

En el caso de que exista un contrato de prestación de servicios por el que se establece un encargado del tratamiento de datos, su identificación estará disponible en el Anexo A.
La duración del contrato de prestación de servicios estará especificada en dicho contrato, pero si por algún motivo no fuese así, se entenderá de duración indefinida, mientras ninguna de las partes decida lo contrario.

Si el encargado del tratamiento presta sus servicios en los locales del responsable del fichero, este último debe asegurarse que el personal del encargado del tratamiento cumple todas las medidas de seguridad previstas en este documento de seguridad. En el caso de que el tratamiento de datos se realizara en los locales del encargado del tratamiento, se deberá reflejar este extremo en el presente documento de seguridad.

Si existieren conexiones remotas a los datos todo el personal del encargado del tratamiento también deberá cumplir las medidas de seguridad establecidas en este documento.

En el caso de documentos en papel o ficheros no automatizados, el responsable del fichero deberá asegurarse de que solamente acceda a ellos el personal autorizado en el Anexo G.

Adicionalmente, el responsable del fichero adoptará las medidas adecuadas para limitar el acceso del personal a datos personales para la realización de trabajos que no impliquen el tratamiento de datos personales.

Salvaguarda y protección de las contraseñas personales.
Sólo las personas relacionadas en el Anexo G, podrán tener acceso a los datos del fichero.

Gestión de soportes.
La salida de soportes informáticos que contengan datos del fichero fuera de los locales donde está ubicado el fichero deberá ser expresamente autorizada por el responsable del fichero. De la misma forma se debe proceder para documentos que contengan datos de carácter personal que vayan a salir fuera del local en que se tratan.

Gestión de incidencias.
El responsable de seguridad habilitará un libro de incidencias a disposición de todos los usuarios y administradores del fichero con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Analizará las incidencias registradas, y deberá tomar las medidas oportunas para procurar que las incidencias queden solucionadas a la mayor brevedad posible.

Procedimientos de respaldo y recuperación.
El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

ADMINISTRADOR DE SISTEMAS

- Función

Serán los responsables de los máximos privilegios y, por tanto, de máximo riesgo de que una actuación errónea pueda afectar al sistema.

Esta figura podrá ser interna si pertenece a la empresa responsable del tratamiento o externa si se contrata un encargado del tratamiento.

Tendrán acceso al software (programa y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

- Obligaciones

Entorno del sistema operativo y de comunicaciones.

Ninguna herramienta o programa de utilidad que permita el acceso al fichero deberá ser accesible a ningún usuario o administrador no autorizado en el Anexo G.

En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos del fichero, como los llamados "queries", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados relaciones en el Anexo G.

El administrador deberá responsabilizarse de guardar en lugar seguro las copias de seguridad y respaldo del fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

Si la aplicación o sistemas de acceso al fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabadas copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

Estos ficheros temporales deben ser borrados cuando dejen de ser necesarios para los fines que motivaron su creación.

En el caso de copias de trabajo de documentos, éstas solamente estarán a disposición del personal autorizado y deberán ser destruidas cuando no sean ya necesarias para el fin para el que hayan sido creadas.

Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al fichero, el administrador responsable del sistema deberá asegurarse de que este acceso no se permita a personas no autorizadas.

Sistema informático o aplicaciones de acceso al fichero.

Si la aplicación informática que permite el acceso al fichero no cuenta con un control de accesos, deberá ser el sistema operativo donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

Salvaguarda y protección de las contraseñas personales.

Las contraseñas se gestionarán mediante el mecanismo que se determina en el Anexo I. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas. En ningún caso el tiempo máximo de cambio de las contraseñas será superior a un año.

Mientras estén vigentes, las contraseñas se guardarán de forma ininteligible. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

USUARIOS DEL FICHERO

- **Función**

Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del fichero, ya que su actuación no precisa de dicho acceso.

- **Obligaciones**

Puestos de trabajo.
Los puestos de trabajo incluidos en el Anexo D estarán bajo la responsabilidad de algún usuario autorizado contenido en el Anexo G que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse con un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

En ficheros no automatizados o documentos, cuando el responsable del puesto deba ausentarse, deberá asegurarse de que los documentos que esté utilizando se guarden en sitio seguro lejos del alcance de personas no autorizadas a acceder a ellos.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el libro de incidencias.

Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración en sus aplicaciones y sistemas operativos que sólo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados del Anexo G.

Salvaguarda y protección de las contraseñas personales.
Cada usuario será responsable de la confidencialidad de su contraseña, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

Gestión de incidencias.
Cualquier usuario que tenga conocimiento de una incidencia es responsable de su comunicación o, en su caso, de su registro en el registro de incidencias del fichero.

El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad del fichero por parte de ese usuario.

Gestión de soportes.
Los soportes que contengan datos del fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del fichero que no estén por tanto relacionadas en el Anexo G.

PROCEDIMIENTOS DE SEGURIDAD

- Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores que contienen el fichero y, en su caso, los documentos o ficheros no automatizados, deben ser objeto de especial protección garantizando la disponibilidad y confidencialidad de los datos protegidos, especialmente si el fichero está ubicado en un servidor con acceso a través de una red.

Deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del fichero o documento que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

La descripción de esos medios se encuentra detallada por cada local en el Anexo C.

- Puestos de trabajo o equipos

Son todos aquellos dispositivos desde los cuales se puede acceder a los datos del fichero, como, por ejemplo, terminales y ordenadores personales.

Se consideran también puestos de trabajo aquellos terminales de administración del sistema, como por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del fichero.

Los procedimientos de seguridad aplicables a los mismos están implícitos en las obligaciones de los usuarios y administradores detalladas anteriormente.

- Entorno de sistema operativo y de comunicaciones

Aunque el método establecido para acceder a los datos protegidos del fichero es el sistema informático referenciado en el Anexo E, al estar el fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos del fichero.

Los procedimientos de seguridad aplicables a los mismos están implícitos en las obligaciones de los usuarios y administradores detalladas anteriormente.

- Sistema informático o aplicaciones de acceso al fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del fichero, y que son usualmente utilizados por los usuarios para acceder a ellos.

Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al fichero o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

Los sistemas informáticos de acceso al fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

Todos los usuarios autorizados para acceder al fichero, relaciones en el Anexo G, deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

Si la aplicación informática que permita el acceso al fichero no cuenta con un control de acceso, deberá ser el sistema operativo donde se ejecuta esa aplicación el que impida el acceso no autorizado, mediante el control de los citados códigos de usuarios y contraseñas.

Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso a los mismos se utilizasen datos reales, se deberá aplicar a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo fichero.

- Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos y deben, por tanto, estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

Sólo las personas relacionadas en el Anexo G podrán tener acceso a los datos del fichero.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el Anexo I.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

GESTIÓN DE INCIDENCIAS

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un Registro de las incidencias que comprometan la seguridad de un fichero o documento es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

El responsable de seguridad del fichero habilitará un libro de incidencias, que estará a disposición de todos los usuarios y administradores del fichero con el fin de que se registre cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma en el Registro de Incidencias del fichero o, en su caso, de su comunicación por escrito al responsable de seguridad o al responsable del fichero. El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del fichero por parte de ese usuario. La notificación o registro de una incidencia se realizará cumplimentando el formulario del Anexo J.

En el supuesto de que una persona no relacionada en el Anexo G deba acceder al sistema informático para solventar una incidencia no prevista como errores, cortes, incidencias técnicas de cualquier tipo que detengan la producción, se dejará constancia identificando al personal técnico y anotándolo en el Registro de Incidencias (Anexo L).

De igual forma se debe actuar si, por algún motivo, alguna persona no relacionada en el Anexo G tenga que acceder al dispositivo de almacenamiento de documentos (ficheros no automatizados).

En el Registro de Incidencias deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

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

GESTIÓN DE SOPORTES

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como DVDs, dispositivos portátiles, etc. son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos tiene el control de estos medios.

Los soportes que contengan datos del fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

En el caso de ficheros que contengan datos que se consideren especialmente sensibles, el etiquetado de los soportes se tiene que realizar utilizando un sistema comprensible y con significado que permita a los usuarios con acceso autorizado identificar su contenido y que dificulte la identificación para el resto de personas.

En el caso de que se vaya a desechar cualquier documento o soporte que contenga datos de carácter personal se deberá proceder a su destrucción o borrado adoptándose las medidas necesarias para evitar accesos indebidos a la información o su recuperación posterior.

Aquellos medios que sean reutilizables, y que hayan contenido copias de datos de los ficheros deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Los soportes que contengan datos del fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del fichero que no estén por tanto relacionadas en el Anexo G.

La salida de soportes informáticos, dispositivos portátiles o documentos que contengan datos de carácter personal, incluidos los comprendidos y/o adjuntos a correos electrónicos, fuera de los locales donde están ubicado los ficheros, ya sea para traslado o para tratar datos fuera de los locales del responsable de los ficheros, deberá ser expresamente autorizada por el citado responsable de los ficheros. Se utilizará para ello el documento adjunto en el Anexo K, debiendo en todo caso garantizarse el nivel de seguridad correspondiente.

En el transporte de soportes se deben adoptar medidas para evitar la sustracción, pérdida o acceso indebido a la información.

Se deben cifrar los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de los locales del responsable de los ficheros.

Consecuentemente, debe procurar evitarse el tratamiento de datos en dispositivos portátiles que no permitan cifrado de datos. En caso de estricta necesidad se podrá realizar mediante la autorización del responsable del fichero, documento adjunto en el Anexo K, y se adoptarán las medidas necesarias para tener en cuenta el tratamiento de datos en entornos desprotegidos.

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN

La seguridad de los datos personales del fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del fichero.

Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo.

Estas copias deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

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

En caso de fallo del sistema con pérdida total o parcial de los datos del fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del fichero al estado en que se encontraban en el momento del fallo.

Únicamente en el caso de que el fallo afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos.
Ese procedimiento está descrito en el Anexo I.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el Registro de Incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

CONTROLES PERIÓDICOS DE VERIFICACIÓN DEL CUMPLIMIENTO

La veracidad de los datos contenidos en los anexos de este documento, así como el cumplimiento de las normas que contienen, deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

El responsable de seguridad del fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados del Anexo G se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al fichero, para lo que

recabará la lista de usuarios y sus códigos de acceso al administrador o administradores de sistemas. Además de estas comprobaciones periódicas, el administrador comunicará al responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al fichero.

Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo que permitan la recuperación del fichero según lo estipulado en el Anexo I.

A su vez, y también con periodicidad al menos trimestral, los administradores del fichero comunicarán al responsable de seguridad cualquier cambio que se haya realizado en los datos técnicos de los Anexos B, D, E y F como, por ejemplo, cambios en el software o hardware, estructura del fichero o aplicación de acceso al fichero, procediendo igualmente a la actualización de dichos anexos.

REGISTRO DE ACCESOS

- Acceso físico

Se registrarán los accesos a los locales donde se encuentre el fichero de aquellas personas no autorizadas explícitamente (mantenimiento, visitas, etc.)

Se registrará, además, el acceso del personal autorizado en el Anexo G fuera de su jornada laboral.

FICHEROS NO AUTOMATIZADOS

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

Los responsables del tratamiento o de los ficheros no automatizados y/o los encargados del tratamiento deberán implantar las medidas de seguridad adecuadas en función del nivel de seguridad exigible al documento o fichero no automatizado.

CRITERIOS DE ARCHIVO

El responsable del fichero debe garantizar que el archivo de los soportes o documentos se realice de manera que se garantice la correcta conservación y gestión de todos los documentos. Se debe tener la opción de poder localizar y consultar de manera sencilla y en todo momento toda la información almacenada.

El establecimiento de una organización de la documentación de forma clara permitirá poder cumplir con la obligación legal de facilitar, a las personas interesadas que así lo soliciten, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación del tratamiento de los datos de carácter personal.

El responsable del fichero deberá revisar o hacer revisar periódicamente, al menos una vez al año, la situación de los documentos archivados para comprobar el correcto estado de los mismos, así como determinar la necesidad de llevar a cabo acción alguna para mantener, entre otros, la integridad de los documentos o el orden lógico de la documentación.

DISPOSITIVOS DE ALMACENAMIENTO

Los dispositivos de almacenamiento de los documentos, generalmente archivadores, armarios, cajas o similares, que contengan datos de carácter personal, deberán estar provistos de una cerradura o algún sistema similar que dificulte la apertura de los mismos.

Si las características físicas de los dispositivos de almacenamiento no permiten dotarlo de cerradura o sistema alguno de apertura controlada, el responsable del fichero o tratamiento, o la persona autorizada por éste, deberá impedir el acceso de personas no autorizadas al armario, archivador o dispositivo en general.

Es recomendable que los armarios, archivadores, cajas u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal se encuentren en áreas que dispongan de puertas dotadas de llave u otro dispositivo similar, y que éstas permanezcan cerradas si no se requiere el acceso a los documentos.

CUSTODIA DE LOS SOPORTES

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento o archivadores, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá proceder a su custodia e impedir, en todo momento, que cualquier persona no autorizada pueda ser acceder a dicha documentación.

El responsable del fichero deberá conocer en todo momento el estado de esta documentación y, en caso de que se produzca alguna incidencia, deberá serle comunicada con la mayor rapidez posible para que se puedan decidir las correcciones o medidas a adoptar en cada caso.

COPIA O REPRODUCCIÓN

Se recomienda vigilar el destino de copias realizadas mediante impresiones, escaneados, etc. y de copias desechadas para que nadie no autorizado acceda a esta documentación.

ACCESO A LA DOCUMENTACIÓN

Si el responsable del fichero lo considerara oportuno, se establecerá algún tipo de control para el acceso de personas a los documentos almacenados.

TRASLADO DE DOCUMENTACIÓN

Es recomendable que si se procede al traslado físico de la documentación contenida en un fichero, se adopten medidas dirigidas a controlar el acceso o manipulación de la información objeto de traslado.

Documento de seguridad de: Página web/ Correo electrónico

Tipo de Solicitud	
[1] Inscripción de creación de fichero	Página web/ Correo electrónico
[ ] Inscripción de modificación de fichero	
[ ] Inscripción de supresión de fichero	Código de inscripción 2141501382

0 Persona física que actúa en representación del responsable del fichero ante la AEPD

Datos del responsable del fichero Razón social o nombre y apellidos RÓTULOS RODRÍGUEZ S.L.			CIF / NIF B82181462
Declarante Nombre LAURA	Primer apellido HERNANDEZ	Segundo apellido AUMENTE	
NIF 47283382M	Cargo o condición del firmante en relación con el responsable del fichero AUTORIZADO POR EL RESPONSABLE		
Dirección a efectos de notificación Razón social o nombre y apellidos GRUPO ADAPTALIA LEGAL FORMATIVO SL Dirección postal CL GOYA, 115, BAJO			
Localidad MADRID	CP 28009	Provincia MADRID	País ESPAÑA
Teléfono 915533408	Fax 915544392	Correo electrónico administracion@grupoadaptalia.es	

1 Datos del responsable del fichero

Nombre o razón social del responsable del fichero RÓTULOS RODRÍGUEZ S.L.			Actividad OTRAS ACTIVIDADES.
CIF / NIF B82181462	Domicilio social CL SEGOVIA 1 POSTERIOR, ,		
Localidad ALCORCÓN	CP 28922	Provincia MADRID	País ESPAÑA
Teléfono 916441764	Fax	Correo electrónico rotulos@rotulosrodriguez.com	

2 Derechos de oposición, acceso, rectificación y cancelación

Nombre de la oficina o dependencia			
CIF / NIF	Dirección postal / apdo. de correos , ,		
Localidad	CP	Provincia	País
Teléfono	Fax	Correo electrónico	

4 Encargado del tratamiento

Nombre y apellidos o razón social				
CIF / NIF	Dirección postal , ,			
Localidad		CP	Provincia	País
Teléfono	Fax	Correo electrónico		

5 Identificación y finalidad del fichero

Denominación Nombre del fichero o tratamiento Página web/ Correo electrónico	Código de inscripción 2141501382
Descripción detallada de finalidad y usos previstos Gestion administrativa de la web de la empresa. Base de datos de acceso a web para adquisicion de productos mediante identificacion personal. **Tipificación correspondiente a la finalidad y usos previstos** Finalidades	
Publicidad y prospección comercial Comercio electrónico Otras finalidades	

6 Origen y procedencia de los datos

Origen [X] El propio interesado o repres. [ ] Registros públicos	[ ] Otras personas físicas [ ] Entidad privada	[ ] Fuentes accesibles al público [ ] Administraciones públicas
Colectivos o categorías de interesados Categoría de colectivos Clientes y usuarios		

7 Tipos de datos, estructura y organización de ficheros

Datos especialmente protegidos			
[ ] Ideología	[ ] Afiliación sindical	[ ] Religión	[ ] Creencias
Otros datos especialmente protegidos			
[ ] Origen racial o étnico	[ ] Salud	[ ] Vida sexual	
Datos de carácter identificativo			
[ ] NIF / DNI [X] Dirección [ ] Imagen / voz	[ ] Nº SS / Mutualidad [X] Teléfono [ ] Marcas físicas	[X] Nombre y apellidos [ ] Firma (man./dig.) [ ] Firma electrónica	[ ] Tarjeta sanitaria [ ] Huella (dact./plan.) [ ] Datos biométricos
Otros datos de carácter identificativo			
Otros tipos de datos			
Correo electronico			

Sistema de tratamiento		
[ ] Automatizado	[ ] Manual	[X] Mixto

8 Medidas de seguridad

Nivel de seguridad	Fecha de auditoria	Tipo de auditoria
[X] Nivel básico [ ] Nivel medio [ ] Nivel alto		

9 Cesión o comunicación de datos

Categoría de destinatarios	

10 Transferencias internacionales

Países sin nivel de protección adecuado	
Países	Categoría de destinatarios

11 Supresión del fichero

Denominación
Código de inscripción
2141501382
Motivo de la supresión

Destino de la información y previsiones adoptadas para su destrucción

Anexo C: Ficha local

Responsable

B82181462 RÓTULOS RODRÍGUEZ S.L.

Fichero

Página web/ Correo electrónico

Código local 0001

Descripción del local

LOCAL

Ubicación física

CALLE GUIPUZCOA 7 LOCAL 8 ▫28922 ALCORCÓN (MADRID)

Equipamiento de seguridad (armarios ignífugos, cerraduras, alarmas, etc.,…)

PUERTA METÁLICA

Anexo C: Usuarios acceso local

Responsable:	1358	RÓTULOS RODRÍGUEZ S.L.
Fichero:	0007	Página web/ Correo electrónico
Local:	0001	LOCAL

Código	N.I.F.	Nombre usuario
0001		GERENCIA

Anexo D: Ficha puesto de trabajo

Responsable

B82181462 RÓTULOS RODRÍGUEZ S.L.

Fichero

Página web/ Correo electrónico

Código puesto de trabajo 0001

Descripción del puesto EQUIPO 1 - GERENCIA

Local de ubicación

Descripción general del puesto

GERENCIA

Descripción del hardware

Sistema operativo

Seguridad

[X] Acceso a Internet	[ ] Módem	[X] Correo electrónico
[X] Uso de contraseñas	[ ] Ficheros temporales	[ ] Cifrado de datos
[ ] Auditoría de accesos	[ ] Prot. pantalla contraseñas	[ ] Auditoría de acciones
[ ] Limitación de intentos		

Otros

Sistema de copia de seguridad integrado

Anexo D: Usuarios acceso equipo

Responsable:	1358	RÓTULOS RODRÍGUEZ S.L.
Fichero:	0007	Página web/ Correo electrónico
Equipo:	0001	EQUIPO 1 - GERENCIA

Código	N.I.F.	Nombre usuario
0001		GERENCIA

Anexo G: Ficha usuario

Responsable

B82181462 RÓTULOS RODRÍGUEZ S.L.

Fichero

Página web/ Correo electrónico

Código usuario	0001
N.I.F.	
Nombre y apellidos	GERENCIA
Cargo	GERENCIA
Departamento	GERENCIA
Equipo	EQUIPO 1 - GERENCIA
Fecha de baja	- -

Privilegios

[X] Creación [X] Modificación [X] Borrado [X] Lectura

Funciones

-Utilización de los equipos de acceso al fichero en su trabajo habitual.
Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las aplicaciones de gestión disponibles.

Anexo G: Accesos del usuario

Responsable:	1358	RÓTULOS RODRÍGUEZ S.L.
Fichero:	0007	Página web/ Correo electrónico
Usuario:	0001	GERENCIA

Código	Descripción
	ACCESO A PUESTOS DE TRABAJO
0001	EQUIPO 1 - GERENCIA
	ACCESO A LOCALES
0001	LOCAL

Anexo H: Documento de confidencialidad

Nombre responsable	RÓTULOS RODRÍGUEZ S.L.
Nombre del fichero	Página web/ Correo electrónico

Código de usuario 0001 **N.I.F.**

Nombre y apellidos GERENCIA

Por el presente documento declara que conoce y acepta las obligaciones que se especifican en el documento de seguridad en el apartado FUNCIONES Y OBLIGACIONES DEL PERSONAL

Y RECONOCE

Que de conformidad con lo dispuesto en el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y los artículos 91 y 94 del R.D. 1720/2007 de 21 de diciembre, sobre medidas de seguridad en acceso a datos de carácter personal de ficheros automatizados, en el caso de que las funciones que desarrolle o los trabajos que realice conlleven realizar tratamientos en ficheros que contengan datos de carácter personal o simplemente su alta como usuario del sistema informático, adquiere el compromiso de utilizar las transacciones con los fines exclusivos de gestión para los que sea autorizado y está obligado a guardar el secreto profesional sobre los datos que tenga conocimiento, siendo responsable de todos los accesos que se realicen a los ficheros informáticos o manuales mediante su contraseña personal y el código de acceso facilitado.

Que ha recibido la parte del documento de seguridad que le corresponde o, en su defecto tiene acceso a dicho documento, y por ello, conoce las normas de seguridad que afectan al desarrollo de sus funciones.

Que el incumplimiento de las obligaciones indicadas, el acceso a la información por usuario no autorizado, la asignación de procesos o transacciones no necesarios para la función encomendada y la falta de custodia o secreto de la identificación personal de acceso, dará lugar a la exigencia de responsabilidades administrativas, en concreto las establecidas en el Titulo VII de la L.O. 15/99 de 13 de diciembre, así como a responsabilidades de cualquier otra naturaleza, incluso penales.

Y ACEPTA LAS SIGUIENTES FUNCIONES

-Utilización de los equipos de acceso al fichero en su trabajo habitual.
Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las aplicaciones de gestión disponibles.

FECHA: FIRMADO: GERENCIA

Anexo I: Contraseñas

Nombre responsable	RÓTULOS RODRÍGUEZ S.L.
Nombre del fichero	Página web/ Correo electrónico

Periodicidad de cambio de contraseñas

ANUAL

Método de distribución

VERBAL

Periodicidad de elaboración

ALFANUMÉRICAS Y NO SE CAMBIA EL FORMATO NUNCA

Anexo I: Copias de seguridad

Definición método

DROPBOX

Definición recuperación copia de seguridad

Periodicidad

Soporte

Formato

Sistema operativo

Anexo J: Impreso de notificación de incidencias

Nombre responsable	RÓTULOS RODRÍGUEZ S.L.
Nombre del fichero	Página web/ Correo electrónico

Incidencia nº _____ (A ser rellenado por el responsable de seguridad)

Descripción detallada de la incidencia

Fecha de notificación - -

Fecha y hora en que se produjo la incidencia - - :

Persona que realiza la notificación

Persona a quien se comunica

Efectos que puede producir (en caso de no subsanación o independientemente de ella)

Persona que realiza la comunicación

Firma.

Anexo J: Impreso de notificación de incidencias (continuación)

Incidencia nº _____ (A ser rellenado por el responsable de seguridad)

Datos resolución incidencias

Fecha de resolución - -

Medidas adoptadas

Resultado de las medidas

Recuperación de datos

Procedimiento realizado

Fecha de realización - -

Datos recuperados

Datos grabados manualmente

Usuario que realiza la operación