Unidad Didáctica 4

Ficheros y medidas de seguridad que se han de adoptar en el documento de seguridad

Contenido

1. Ficheros y tratamientos de datos

Se entiende por **tratamiento de datos** las operaciones y procedimientos técnicos de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Este puede ser:

- **Automatizado:** se refiere a todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados, es decir, información almacenada en soportes informáticos y que se encuentran organizados de manera que se pueda acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado.
- **No automatizados:** es todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Además, también pueden ser:

- **Ficheros de titularidad privada:** los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
- **Ficheros de titularidad pública:** los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las enti-

dades u organismos vinculados o dependientes de las mismas y las corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

Los ficheros de datos de carácter personal de titularidad privada, serán notificados a la Agencia de Protección de Datos.

La notificación de inscripción de los ficheros a la Agencia de Protección de Datos ha de contener:

- Identificación del responsable del fichero.
- La identificación del fichero.
- Finalidades y usos del fichero.
- El sistema de tratamiento empleado para su organización.
- El colectivo de personas sobre las que se obtienen datos.
- El procedimiento y procedencia de los datos.
- Las categorías de los datos.
- El servicio o unidad de acceso.
- La indicación del nivel de medidas de seguridad básico, medio o alto exigible.
- Identificación en su caso del encargado de tratamiento donde se encuentra ubicado el fichero
- Los destinatarios de cesiones y transferencias internacionales de datos.

2. El responsable del fichero y el encargado del tratamiento

Dentro de la LOPD podemos distinguir a dos agentes principales:

- **Responsable del fichero o tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. Además, es el responsable de elaborar e implantar el Documento de Seguridad, el cual recoge toda la normativa referente a la seguridad de los datos y a los sistemas de información.

- **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

El servicio prestado por el encargado del tratamiento puede tener o no carácter remunerado y ser temporal o indefinido.

Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte el tratamiento de datos de carácter personal, deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento del servicio encomendado.

La realización de tratamiento por cuenta de terceros debe estar regulada en un contrato que debe constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el supuesto de que el encargado incumpliese lo mencionado anteriormente, será considerado también responsable del tratamiento, y responde de las infracciones en las que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no es responsable cuando por indicación expresa del responsable del fichero, comunique datos a un tercero designado por aquél, al que se le hubiera encomendado la prestación de un servicio conforme a lo que se establece en el contrato.

El encargado del tratamiento no puede subcontratar con un tercero la realización de ningún tratamiento, salvo que hubiera obtenido la autorización del responsable del fichero. En este caso, la contratación se efectuará en nombre y por cuenta del responsable del fichero.

Existen excepciones a la imposibilidad de subcontratar con un tercero la realización de tratamientos, es decir, es posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan unos requisitos:

- Que especifique en el contrato de servicios que puedan ser objeto de subcontratación y, si fuera posible, la empresa con la que se vaya a subcontratar.
- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajusta a las instrucciones del responsable del fichero.
- Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos anteriormente.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el **artículo 20.3 del reglamento**.

El encargado del tratamiento debe conservar los datos. Una vez cumplida la prestación contractual, los datos personales deben ser destruidos o devueltos al responsable del tratamiento o al encargado que hubiese designado. No se procede a la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso debe proceder a la devolución de los mismos, garantizando el responsable del fichero dicha conservación.

Ejemplo

El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan, a un encargado de tratamiento que preste sus servicios en los locales del primero, debe hacerse constar esta circunstancia en el Documento de Seguridad de dicho responsable, comprometiéndose el personal del encargado a cumplir las medidas de seguridad contenidas en el mismo.

Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, anejos a los del responsable del fichero, debe elaborar un documento de seguridad en los términos exigidos, en el artículo 88 del reglamento, o completar el que ya hubiera elaborado, en su caso, identificando el fichero o

tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. Medidas y documento de seguridad

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

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

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

NIVEL BÁSICO
- Nombre - Apellidos - Datos de contacto (dirección, teléfono, e-mail...) - Cualquier otro dato que no sea nivel medio o alto.
NIVEL MEDIO
- Datos relativos a la comisión de infracciones administrativas o penales - Datos de los que sean responsables las Administraciones tributarias - Datos de los que sean responsables las entidades financieras - Datos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social - Datos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas - Datos que ofrezcan una definición de las características o personalidad de los ciudadanos y permitan evaluar aspectos de su personalidad o comportamiento.
NIVEL ALTO
- Ideología - Afiliación sindical - Religión y creencias - Origen racial - Salud y vida sexual - Datos recabados para fines policiales sin consentimiento de las personas afectadas - Datos derivados de actos de violencia de género.

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

3.1. Medidas de seguridad aplicables a ficheros y tratamientos automatizados

A continuación vamos a ver las medidas de seguridad que se aplican a cada tipo de fichero y a los tratamientos automatizados según el nivel de seguridad ante el que nos encontremos.

Medidas de seguridad de nivel básico

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. Esto lo prevé el **artículo 81.1 del R. D. 1720/2007 de 21, de diciembre que desarrolla la Ley orgánica 15/1999 de protección de datos.** Lo que pretende es que cualquier dato personal esté protegido con medidas de Seguridad. Las medidas de nivel básico se desarrollan en el Título VIII en su Capítulo I y son las siguientes:

Funciones y obligaciones del personal

En dicho título aparece el texto siguiente:

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

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento (art. 89 del R. D. 1720/2007). La realización de una formación específica (ya sea en su modalidad presencial u online), o la

difusión entre los empleados de la normativa, procedimientos, e implicaciones para que los empleados estén al corriente. La empresa debería considerar la necesidad de obtener formalmente la aceptación de las normas y procedimientos por parte de sus empleados, La finalidad de esta medida, es evitar la ilegalidad en el tratamiento de datos por parte de la plantilla.

Les mostramos la plantilla que deberá entregarse al personal para que conozca sus obligaciones respecto a la protección de datos.

OBLIGACIÓN DEL DEBER DE SECRETO PERSONAL

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

Por ello, D. /Dª (NOMBRE TRABAJADOR), se compromete a guardar secreto sobre todo los datos de carácter personal y cualquier información o circunstancias a los que haya tenido acceso, en el ejercicio de las funciones que le hubiesen sido asignadas. Las anteriores obligaciones se extienden a cualquier fase del tratamiento de los citados datos, y subsistirán aún después de concluidas las funciones en el marco en los cuales ha tenido acceso a los datos o concluida su vinculación con (NOMBRE DE LA EMPRESA)

Registro de incidencias.

El artículo 90 dice lo siguiente:

> *Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.*
>
> (Art. 90 del R. D. 1720/2007)

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

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

Lo cierto es que no llevar ese registro significa un incumplimiento de la Ley de Protección de Datos. Y son muchas las empresas que la incumplen por culpa de no llevar este registro de incidencias y que por tanto están expuestas a una sanción por parte de la Agencia de Protección de Datos.

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

- Modificaciones/accesos no autorizados de información.
- Pérdida de información.
- Copias indebidas de datos en los puestos de trabajo.
- Mal funcionamiento durante la realización de copias de seguridad.

- Accesos no autorizados a las salas donde se ubiquen los sistemas y soportes informáticos (oficina, caja de seguridad, etc.).
- Intento no autorizado de salida de soportes.
- Destrucción total/parcial de soportes físicos.
- Conocimiento por terceros del identificador de usuario y contraseña.
- Existencia de sistemas sin las debidas medidas de seguridad.

A continuación, les mostraremos un modelo de notificación de incidencias.

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

Modelo de notificación de incidencias

Control de acceso

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

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

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

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

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

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

Identificación y autenticación

El reglamento de la Ley establece que el responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer los procedimientos de identificación y autenticación necesarios para dichos accesos,

es decir, disponer de mecanismos adecuados que impidan el acceso de usuarios no autorizados al sistema.

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

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

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

En el caso de las contraseñas, se debe asegurar que las mismas sean robustas, que no sean fácilmente deducibles, y que no estén a la vista del resto de empleados. Es conveniente fijar unos requisitos que deben cumplir las cadenas utilizadas como contraseña (longitud mínima, combinación de caracteres alfanuméricos…).

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

Gestión de soportes y documentos

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

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

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

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

En el supuesto de que hubiera que desechar cualquier documento o soporte que contenga datos de carácter personal, se procederá a su destrucción o borrado, siempre tomando las medidas necesarias para evitar el acceso a la información contenida en el mismo o su posterior recuperación.

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

Ejemplo

Fecha de actualización: 31 de enero de 2012.

Identificador del soporte: NOM-31012012

Descripción del soporte: copia de seguridad de los datos de nóminas de los empleados de la empresa a fecha de 31 de diciembre de 2007.

Continúa en página siguiente >>

<< Viene de página anterior

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

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

Copias de Respaldo y recuperación

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

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

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

- Como mínimo se deben realizar semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.
- Hay que establecer procedimientos que garanticen la recuperación de los datos que aseguren en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el supuesto de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad, con la finalidad de poder realizar las copias de respaldo y recuperación que facilitarán que los datos estén siempre actualizados y adecuados a la realidad.

- Cada seis meses el responsable del fichero deberá verificar la correcta definición, funcionamiento y aplicación de los procedimientos de realización de las copias de respaldo y de recuperación de datos (ver que se hacen bien, que copian lo que deben y comprobar que se restauran correctamente).
- Si se van a cambiar o modificar los sistemas de gestión que tratan los datos, las pruebas que se realicen no podrán efectuarse con datos reales a no ser que se garanticen las medidas de seguridad aplicables y se anote en el documento de seguridad. Si así se hace, habrá que realizar una copia de seguridad previa (artículo 94. R. D. 1720/2007).

Medidas de seguridad de nivel medio

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

Responsable de seguridad

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

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

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

Auditoría

La normativa actual determina la obligación de realizar una auditoria bienal a partir del tratamiento de ficheros automatizados y no automatizados de nivel medio. Esto implica la necesidad de someterse, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad previstas en el RDLOPD.

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

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

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

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

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

- Este informe deberá quedar a disposición de la Agencia de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas.

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

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

Gestión de soportes y documentos

También esta medida establece una serie de cuestiones adicionales a su medida análoga del nivel básico:

- Se deberá disponer de un sistema de **registro de entrada** de soportes que permita, directa o indirectamente, conocer las siguientes cuestiones:
  - Tipo de documento o soporte.
  - Fecha y hora de entrada del documento o soporte.
  - El emisor del soporte.
  - El número de documentos o soportes en el envío.
  - El tipo de información que contiene.
  - Forma de envío de los documentos o soportes.
  - Persona que se encarga de la recepción del soporte, persona que debe estar autorizada para ello y debe reflejarse así en el documento de seguridad.

- Además se deberá disponer también de un **registro de salida** de soportes informáticos que nos permita conocer los siguientes aspectos:
  - Tipo de documento o soporte.
  - Fecha y hora de salida del documento o soporte.

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

NOMBRE DE LA EMPRESA	**REGISTRO Y AUTORIZACIÓN DE ENTRADA DE SOPORTES**
Entrada del soporte: 000003	Fecha: Hora:
Soporte	
Tipo de soporte y número	
Contenido	
Fecha de creación	
Origen y finalidad	
Finalidad	
Origen	
Forma de envío	
Medio de envío	
Remitente	
Precauciones para el transporte	
Autorización	
Persona responsable de la recepción	
Cargo \ puesto	
Observaciones	
Firma	

Modelo de registro y autorización de entrada de soportes

Identificación y autenticación: se refuerza la medida de identificación autenticación que se prevé en el nivel de seguridad básico.
El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información, lo que supone bloquear el identificador de usuario después de un número limitado de intentos de acceso.
Lo que se pretende con esta medida de nivel medio es tener a todos los usuarios del sistema controlados, y evitar la posibilidad de un acceso no autorizado a los datos (artículo 98 del R. D. 1720/2007).
Control de acceso físico: se pretende establecer medidas físicas para garantizar un control de acceso a los locales donde se ubiquen los sistemas de información con datos personales. Los usuarios que pueden acceder físicamente a estos lugares deben de identificarse en el documento de seguridad (artículo 99 del R. D. 1720/2007).
Registro de incidencias: esta medida de seguridad establece una serie de cuestiones adicionales a su medida análoga de nivel básico regulada en el art. 90 del reglamento, establece que además de los requisitos establecidos en el mismo, deberán consignar los procedimientos realizados de recuperación de los datos, indicando lo siguiente:

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

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

<table>
<tr><td colspan="2">Empresa</td><td>Impreso de notificación de incidenciast</td></tr>
<tr><td colspan="3">Incidencia nº: 0000002 (a cumplimentar por responsable seguridad)</td></tr>
<tr><td colspan="2">Fecha de notificación:</td><td></td></tr>
<tr><td colspan="2">Tipo de incidencia:</td><td>Fecha y hora en que se produce /detecta *

(* Tachar lo que no proceda)</td></tr>
<tr><td colspan="3">Descripción detallada de la incidencia:</td></tr>
<tr><td colspan="3">Efectos que puede producir: (en caso de no subsanación o incluso independientemente de ella)</td></tr>
<tr><td colspan="3">Recuperación de datos: procedimiento realizado: datos restaurados: datos grabados manualmente:

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

Fecha hora</td><td>Corrección de la anomalía:

Fecha hora</td></tr>
<tr><td colspan="3">¿Se aplican medidas correctoras? Si ☐ NO ☐</td></tr>
<tr><td rowspan="2">Seguimiento</td><td>Descripcion:</td><td>Acciones a realizar:</td></tr>
<tr><td>Comprobación de la eficacia</td><td>Realizada por:

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

Modelo de notificación de incidencias

Medidas de seguridad nivel alto

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

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

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

Gestión y distribución de soportes

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

Siempre que exista una distribución de soportes que contengan datos personales altamente protegidos, la información que contengan estos soportes deberá encontrarse cifrada (existen diferentes técnicas de cifrado de información). Es un método seguro porque a través de una clave se podrá cifrar una información, pero aparecerá en forma de caracteres y símbolos sin sentido, lo que no es más que la información que está cifrada). El artículo 101 del reglamento da libertad a la hora de elegir un

mecanismo para evitar la manipulación de estos datos tan sensibles, por lo que se podrá utilizar cualquier otro mecanismo diferente al cifrado de los datos siempre que se garantice la ininteligibilidad y la no manipulación en el momento en que el soporte se esté transportando. Recomendamos la utilización de las técnicas de cifrado para evitar las complicaciones técnicas, ya que el cifrado se encuentra hoy muy estandarizado y normalizado.

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

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

Copias de respaldo y recuperación

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

Registro de accesos

Lo que pretende esta medida de seguridad de nivel alto es potenciar más aún, las medidas de identificación y autenticación y de control de

accesos de los niveles básico y medio. La encontramos en el art.103 del reglamento.

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

- Identificación del usuario que ha accedido.
- Fecha y hora en que se ha accedido.
- Fichero al que se ha accedido.
- El tipo de acceso:
  - Acceso para consultar datos.
  - Acceso para modificar datos.
  - Acceso para suprimir datos.
  - Acceso para introducir datos.

Si el acceso ha sido autorizado o denegado. Si ha sido autorizado, se deben registrar en este registro de accesos las informaciones necesarias para identificar los datos a los que se ha accedido.

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

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

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

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

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

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

Telecomunicaciones

Para entender las medidas de seguridad, vamos a definir los siguientes conceptos:

- **Telecomunicación:** es toda transmisión, emisión o recepción de signos, señales, escritos, imágenes sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.
- **Red de telecomunicaciones:** son los sistemas de transmisión y los equipos de conmutación y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante cable, medios ópticos o de otra índole. La red de telecomunicaciones más importante es Internet (una red LAN, o lo que es lo mismo, una red interna, que solo opera dentro de un edificio o entre unas oficinas, no se considera una res de telecomunicaciones).

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

Ocurre lo mismo que en la medida de nivel alto referente a la distribución de soportes: no tiene por qué utilizarse el mecanismo del cifrado ya que el legislador da libertad a la hora de elegir un mecanismo siempre que la ininteligibilidad y la no manipulación de los datos personales estén garantizadas durante la transmisión de estos. Seguimos recomendando las técnicas del cifrado, métodos generalizados hoy en día.

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

Antes de establecer cuáles son las medidas que se han de tomar para proteger la información contenida en los ficheros no automatizados vamos a ofrecerles una definición de los mismos:

Los ficheros no automatizados: *"todo conjunto de datos de carácter personal organizado de forma no automatizado (en papel), 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".*

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

Ejemplo

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

Medidas de nivel Básico

El nuevo reglamento incluye en su ámbito de aplicación a los ficheros automatizados (papel), estableciendo su regulación en el capítulo IV. Además de las medidas de seguridad establecidas en este capítulo, se deben aplicar las

disposiciones comunes dispuestas en los capítulos I y II del Reglamento destinadas tanto para ficheros automatizados como no automatizados y por último deben aplicarse las medidas de seguridad de nivel básico para los ficheros automatizados en cuanto a:

a. Funciones y obligaciones del personal.
b. Registro de incidencias.
c. Control de acceso.
d. Gestión de soportes.

Las medidas propias o específicas de este tipo de ficheros son las siguientes:

Criterios de archivo

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

Para determinar dichos criterios de archivo deberá estarse, en primer lugar, a los previstos en la legislación específica que pueda regular determinados tipos de ficheros (como puede ser el caso del archivo de facturas, los libros de los registros civiles o las historias clínicas). Cuando no exista ninguna normativa aplicable, deberá ser el propio responsable del fichero quien establezca los criterios y procedimientos de actuación que deban seguirse para el archivo (artículo 106 del R. D. 1720/2007).

Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura, lo que se traduce en la necesidad de que todos aquellos armarios, archivadores, cajones y demás dispositivos análogos en los que vayan a guardarse este tipo de documentos estén provistos de cerraduras

con llave o de cualquier otra medida de cierre similar (artículo 107 R. D. 1720/2007).

Si las características físicas de dichos dispositivos de almacenamiento no permiten adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas a la documentación, para evitar que dicha información sea utilizada o manipulada para fines distintos para los que se obtuvieron.

Custodia de soportes

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

Medidas de seguridad de nivel medio

Para implantar las medidas de nivel medio es necesario adoptar las siguientes disposiciones:

El responsable de Seguridad

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

Auditoría

Los ficheros no automatizados también deben someterse a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad que les son aplicables y que, como mínimo, deberá realizarse

cada dos años. Como es lógico, en una misma auditoría pueden revisarse tanto los ficheros automatizados como los no automatizados, no siendo necesaria la realización de dos auditorías separadas.

La Auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización, y evitar que se puedan manipular o dar un uso distinto a los datos contenidos en este tipo de ficheros.

Medidas de seguridad de nivel alto

Aquellos ficheros no automatizados que contengan datos de nivel alto, además de las medidas de seguridad de nivel básico y medio ya vistas, deberán someterse también a las siguientes:

Almacenamiento de la información

Cuando los ficheros no automatizados contengan datos de nivel alto, el Reglamento de Protección de Datos establece que los armarios, archivadores u otros elementos en los que estos se almacenen deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

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

Copia o reproducción

En este nivel de seguridad, la generación de copias o la reproducción de los documentos únicamente podrá realizarse bajo el control del personal autorizado para ello en el documento de seguridad, por lo que se

restringe la posibilidad de que puedan darse copias no controladas de la documentación con datos especialmente sensibles.

Por otro lado, la destrucción de dichas copias o reproducciones deberá realizarse de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. Así, para el correcto cumplimiento de esta medida se recomienda el uso de destructoras de papel, o bien, para elevados volúmenes de documentación desechada, la contratación de un servicio de recogida y destrucción de papel correctamente gestionado (artículo 112 del R. D. 1720/2007).

Acceso a la documentación

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

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

Traslado de documentación

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

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

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

Las disposiciones comunes a ambos ficheros son las que aparecen a continuación.

Documento de Seguridad

Concepto

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

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

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

Estructura y contenido

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

- Ámbito de aplicación del documento de seguridad con especificación detallada de los recursos protegidos.

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

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

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

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

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

El contenido del Documento de Seguridad debe adecuarse a los cambios de las leyes o reglamentos en esta materia de seguridad de los datos personales. El documento debe mantenerse siempre actualizado y se tiene que revisar siempre que haya cambios importantes en el sistema de información o la organización del sistema de información.

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

Control del cumplimiento

De nada serviría disponer de un documento de seguridad casi perfecto si no se controla que, efectivamente, lo que se indica en el mismo por un lado cumple lo que dispone el Reglamento y por otro lado, es lo que se viene realizando en la práctica. Algo que si no llevasen a cabo dichos controles se averiguaría cada dos años al efectuar la auditoria bienal (nivel medio y alto).

Si los controles se establecen correctamente, se convierten en un control interno y se podría decir que hasta en una auditoría continua, con las ventajas que esto conlleva.

Prestación de servicios sin acceso a datos personales

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

Delegaciones de autorizaciones

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

AUTORIZACIÓN

EMPRESA: _____.

Nombre de quien otorga la autorización y NIF_____, cuyas competencias son_____ , autoriza a Nombre de la persona autorizada y NIF_____, desde Fecha_____hasta Fecha_____, a Tipo de autorización_____ con alcance (pleno o parcial) _____.

OBSERVACIONES (si las hubiera): _____

Firma de la persona que otorga la autorización:

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

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

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

En Málaga, a 22 de junio de 2010

REUNIDOS

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

Y de otra parte:

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

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

EXPONEN

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

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

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

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

Continúa en página siguiente >>

<< Viene de página anterior

tratamiento de los datos de carácter personal, la prestación de servicios mencionados, por parte del Encargado de Tratamiento.

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

ESTIPULACIONES

Primera.- Objeto del contrato

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

En ambos supuestos, el Responsable del Fichero facilitará los datos que sean necesarios para la prestación del servicio acordado, y a los que se le dará el tratamiento de los mismos en conformidad con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, y el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Segunda.-Tratamiento de datos de carácter personal.

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

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

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

Cuarta.- Finalidad del tratamiento

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

Continúa en página siguiente >>

<< Viene de página anterior

Quinta.- Medidas de Seguridad

El Encargado de Tratamiento deberá aplicar a los datos contenidos en los Ficheros, las medidas de seguridad establecidas reglamentariamente en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, para así garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

Sexta.- Comunicación de Datos a Terceros

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

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

Séptima.- Ejercicio de derechos.

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

Octava.-Deber de información mutuo.

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

Novena.- Deber de conservación.

El Encargado de Tratamiento conservará los datos de carácter personal a los que haya tenido acceso en razón del servicio prestado, así como cualquier soporte o documento en el que consten, durante el tiempo en que esté vigente dicho servicio o porque así lo disponga la Ley. Finalizado éste o resuelto el presente contrato, los datos serán destruidos en su totalidad o devueltos al responsable

Continúa en página siguiente >>

<< Viene de página anterior

del fichero, teniendo en cuenta los distintos soportes o documentos donde estos puedan constar: base de datos en discos, ficheros temporales, copias de seguridad, soportes en papel…etc.

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

Décima.- Responsabilidad

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

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

Décimo primera - Totalidad de pactos y conservación de contrato.

El presente documento contiene todos los pactos que gobiernan la relación jurídica entre ambas partes. Cualquier modificación de los mismos deberá ser acordado previamente por ambas partes, debiéndose suscribir un documento al efecto.

En todo caso, en el supuesto de que alguna de las estipulaciones que se contienen en el mismo fuese anulada por decisión judicial o arbitral, ello no afectará a las demás estipulaciones, manteniéndose el contrato plenamente vigente en todo lo no expresamente declarado nulo o anulado. Asimismo, las estipulaciones declaradas nulas o anuladas serán sustituidas por otras que sean válidas y que recojan, dentro de lo posible, y de la manera más parecida posible, el contenido, de las estipulaciones nulas o anuladas.

Décimo segunda.- Cláusula de confidencialidad

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

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

Continúa en página siguiente >>

<< Viene de página anterior

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

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

Décimo tercera.- Duración y resolución del contrato.

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

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

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

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

_____

EMPRESA S.L. (QUE PRESTA EL SERVICIO)

D./Dª
(Encargado de Tratamiento)

EMPRESAS CLIENTE

D./Dª.
(Responsable del Fichero)

Creación de ficheros temporales o copias de trabajo de documentos

Son aquellos que se han creado exclusivamente para la realización de trabajos temporales o auxiliares, por ejemplo, (realizar una copia de seguridad temporal ante un corte de suministro que detenga repentinamente el sistema), deberán cumplir el nivel de seguridad que les corresponda conforme a lo establecido en el artículo 81 del reglamento.

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

Ejercicios de repaso y autoevaluación

1. **¿Qué son las medidas de seguridad?**

2. **¿Qué es el documento de seguridad?**

3. **¿Quién tiene la obligación de realizar el Documento de Seguridad?**

4. **Enumere las medidas de seguridad obligatorias que se deben adoptar en ficheros o tratamientos de datos de nivel básico.**

5. **¿Cada cuánto tiempo se han de realizar las copias de respaldo y recuperación de datos en ficheros o tratamientos de nivel básico?**

6. **¿Qué son los ficheros temporales o copias de trabajo?**

7. **¿Quién es el responsable de seguridad del fichero o tratamiento de datos? ¿Cuántos responsables de seguridad se podrán nombrar?**

8. **¿A partir de qué nivel de seguridad debe aparecer o debe crearse la figura del responsable del fichero?**

9. **¿A partir de qué nivel se requerirá la realización de una auditoría? ¿Cada cuánto tiempo habrá de realizarse?**