MANUAL DE USUARIO

Ley de Protección de Datos
De Carácter Personal

ALANA

01/08/2019

INTRODUCCIÓN

La protección de los datos de carácter personal de los ciudadanos ha sido regulada en Europa por el Reglamento General de Protección de Datos 679/2016 y por la legislación estatal, cuyo objeto principal lo constituye la salvaguarda del derecho al honor, la intimidad personal, y la propia imagen de las personas físicas, atribuyen determinadas funciones y obligaciones a todas aquellas personas que intervienen en el tratamiento de los ficheros donde se almacenan los datos de carácter personal.

La Ley impone sanciones económicas muy elevadas a las organizaciones (sanciones que pueden llegar hasta los 20.000.000 euros) y sus efectos en el mercado como la publicidad (negativa) de la sanción, la inmovilización temporal del fichero, los daños reputacionales, … etc.

El objeto de este manual es detallar las funciones y obligaciones que, como usuario de los ficheros con datos de carácter personal de la entidad, tiene que conocer y respetar.

1.- GLOSARIO DE TÉRMINOS

DATOS DE CARÁCTER PERSONAL

Cualquier información concerniente a personas físicas identificadas o identificables. Es decir, cualquier dato que podamos relacionar con personas físicas. En el ámbito de las empresas esas personas serán normalmente potenciales clientes, clientes, proveedores, trabajadores de la empresa, terceros o personas de contacto.

En algunos ámbitos concretos de actividad puede que los datos se refieran a otras personas como pacientes, asociados ...o por ejemplo en el ámbito público dichos afectados son los ciudadanos, contribuyentes etc., además de algunos afectados comunes al ámbito privado: por ejemplo los empleados, proveedores, contactos, etc.

Téngase en cuenta que no sólo se refiere a personas identificadas (cuando tengamos su nombre) sino también cuando esas personas sean razonablemente identificables por ejemplo a través de un identificador: por ejemplo número de colegiado, DNI, IP, correo electrónico, etc.

AFECTADO O INTERESADO

Persona física titular de los datos. Es la persona cuyos datos se tratan, es decir: el cliente, paciente, ciudadano, empleado, proveedor, contacto, etc.

TRATAMIENTO DE DATOS

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Téngase en cuenta que a tenor de la definición de tratamiento que da la ley cualquier operación que se haga con ellos: grabarlos, modificarlos, conservarlos, enviarlos, etc., constituirá tratamiento.

FICHERO

Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Es decir, cualquier dato que tengamos sobre personas físicas en cualquier tipo de soporte, tanto en papel como a nivel informático.

El concepto de fichero no se corresponde necesariamente con una base de datos, sino que siempre que exista un conjunto de datos que estén organizados mediante algún criterio, nos encontraremos ante la existencia de un fichero.

Obviamente una aplicación informática de nóminas constituye un ejemplo de fichero, pero también lo puede constituir una tabla de datos en Word, sin olvidar que también es aplicable este concepto a los datos no automatizados: por ejemplo un archivo A-Z.

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. El responsable del fichero normalmente coincidirá con la organización: la empresa, asociación, institución, empresarios individual, profesional, etc. y es a quien se le imponen la mayoría de las obligaciones en protección de datos siendo, por tanto, normalmente el responsable de las sanciones que - en su caso - se impongan. Ello sin perjuicio de que el responsable del fichero pueda nombrar una persona física que le represente

ENCARGADO DEL TRATAMIENTO

La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento El encargado del tratamiento es un tercero (normalmente una empresa pero no necesariamente) que le presta un servicio al responsable del fichero y que para ello requiere acceder a datos del responsable.

Ejemplos típicos de encargados son la asesoría laboral, contable o fiscal (que acceden a los datos de empleados, clientes o proveedores de su cliente para asesorarle), empresas de mantenimiento de hardware o software, etc.

El servicio que presta el encargado no tiene porqué ser remunerado. La relación entre el responsable y el encargado se debe regular de acuerdo con la legislación vigente.

RESPONSABLE DE SEGURIDAD

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero. El responsable de seguridad puede ser uno o varios y son los encargados de coordinar y controlar las medidas definidas en el documento de seguridad.

En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero, que es a quien en primera instancia se le pueden imponer en su caso las sanciones que contempla la Ley.

Ello es sin perjuicio de que el responsable de seguridad, si no cumple con sus obligaciones, pueda tener responsabilidad laboral o disciplinaria

USUARIO

Sujeto o proceso autorizado a acceder a datos o recursos. Normalmente un usuario será una persona que accede a datos de la organización. El usuario podrá tener diferentes perfiles de acceso y ser un usuario interno o externo (un usuario de otra organización que accede a nuestro sistema para prestar un servicio, por ejemplo mantenimiento informático).

CONSENTIMIENTO

Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernen. Téngase en cuenta que el consentimiento es el eje vertebral de la protección de datos y ello exige que, como regla general, no se puedan tratar datos de nadie sin su consentimiento, sin perjuicio de que en ocasiones esta obligación está exenta. Por ejemplo, cuando los datos se traten en el marco de la relación negocial, laboral o administrativa, cuando exista una Ley que disponga lo contrario, etc.

COMUNICACIÓN DE DATOS

Toda revelación de datos realizada a una persona distinta del interesado. La cesión de datos debe estar, salvo excepciones, necesariamente consentida por el interesado.

Por ello, es importante no comunicar datos de carácter personal a otras personas físicas o jurídicas (ni si quiera a familiares directos), salvo que se disponga del consentimiento expreso de dicha persona o se esté ante alguna de las excepciones previstas por la Ley.

2.- FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

2.1- OBLIGACIONES GENERALES

a. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

b. Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

c. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información titularidad de la organización fuera de los locales de la misma, sin autorización previa del Responsable de Seguridad. En el supuesto de existir traslado o distribución de soportes y documentos se realizará cifrando dichos datos, o mediante otro mecanismo que el acceso o manipulación de la información por terceros.

d. Ficheros de carácter temporal o copias de documentos son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estos ficheros de carácter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán cumplir con los niveles de seguridad asignados por el Responsable de Seguridad.

   Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.

e. Únicamente las personas autorizadas en un listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad correspondiente.

f. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

g. Comunicar, de forma inmediata, al Responsable de Seguridad, cualquier conocimiento de solicitud, por parte de los interesados, de

derechos, acceso, rectificación, supresión (derecho al olvido), limitación de tratamiento, portabilidad de los datos, cancelación y a no ser objeto de decisiones automatizadas.

2.2.- OBLIGACIONES RESPECTO DE LOS FICHEROS AUTOMATIZADOS

a. Cambiar las contraseñas a petición del sistema.

b. Mantener en secreto sus claves de acceso al sistema, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido el secreto.

   Las contraseñas de acceso al sistema son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida

c. Cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

d. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al ordenador personal, disquetes, portátil o a cualquier otro soporte sin autorización expresa del Responsable de Seguridad correspondiente.

e. Guardar todos los ficheros con datos de carácter personal en la carpeta del servidor indicada por el Responsable de Seguridad correspondiente, a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.

f. Cada usuario que mande un listado a una impresora, sea ésta propia o compartida, se deberá asegurar que no quede ningún documento en la bandeja de salida, que contengan datos protegidos. Además deberá retirar los documentos, conforme vayan saliendo, con el fin de evitar que mientras se imprimen, puedan ser leídos por personas no autorizadas.

g. Los usuarios tiene prohibido el envío de información de carácter personal de nivel alto, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

h. El envío de e-mails conteniendo datos personales debe realizarse encriptando previamente la información.

i. Los usuarios no podrán, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador empleado en el puesto de trabajo.

j. **Queda prohibido**:

i) Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

ii) Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad competente.

iii) Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.

iv) Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.

v) Queda prohibido el uso del correo electrónico para fines no relacionados con las funciones laborales encomendadas. El empleo del nombre o apellidos de los trabajadores o funcionarios junto al dominio de la organización en las direcciones de correo no significa la asignación por la organización de un correo personal, esto se realiza únicamente por motivos organizativos internos de asignación de áreas y puestos de trabajo.

vi) Utilizar Internet para tareas que no estén relacionadas directamente con las funciones asignadas al usuario. La organización regulará las modalidades de acceso y las restricciones o limitaciones del mismo. Queda prohibida la descarga de software o ficheros de cualquier tipo desde Internet, sin consentimiento expreso de la organización, y ello aunque resulte de un acceso consentido por motivos de trabajo.

vii) Introducir contenidos en la red corporativa y/o ordenador personal que no guarden relación con la actividad y objetivos de la entidad.

viii) Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

Estas obligaciones sólo serán exigibles a los usuarios de ficheros automatizados, en tanto en cuanto la organización disponga los medios adecuados en cada caso.

2.3.- CON RESPECTO A FICHEROS NO AUTOMATIZADOS (PAPEL)

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

a. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.

b. Mantener debidamente custodiadas las llaves de acceso a las dependencias de la empresa, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de carácter personal, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido esa custodia.

c. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

d. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

e. Queda prohibido el traslado de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información titularidad de la entidad fuera de los locales de la misma.

f. Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

g. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.

h. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad.

2.4.- CON RELACIÓN AL TRABAJO DIARIO

La aplicación de las funciones y obligaciones de todas las personas que tengan acceso a datos, afecta de forma importante el trabajo diario.

Por esta razón, es importante ser consciente de que un error puede acarrear desagradables consecuencias, por lo que antes de cometerlo, es preferible consultar.

El cumplimiento estricto de la Ley de Protección de datos, en el trabajo diario supone:

- **Informar a los interesados antes de proceder a la captura de datos**

  Para ello, se contará con carteles informativos, cláusulas en impresos, folletos informativos, etc., que faciliten esta obligación.

  También se podrá contar con un sello de caucho, donde figure una cláusula reducida para ponerla en aquellos impresos o documentos que no lleven impresa la cláusula informativa.

- **Solicitar la firma del interesado, afirmando que ha sido informado y que autoriza el tratamiento de datos.**

  Aunque no suele haber mucha costumbre que los Clientes, a la hora de encargar un trabajo firmen ningún documento, a partir de ahora, estamos obligados e exigir su firma como demostración de que ha sido informado, según marca la Ley y que da su autorización al tratamiento.

  En el caso de que los datos hayan sido facilitados por el propio interesado, mediante una llamada de teléfono, la entrega de una tarjeta o cualquier otro medio similar, sin que se le haya podido informar correctamente, se deberá preceder a informarle con posterioridad, dándole opción a negarse a la incorporación de los mismos al fichero o al tratamiento de los mismos.

  En estos casos, cuando la persona se persone en la Empresa, se le deberá solicitar la firma.

  Otra forma, sería el envío de una carta o correo electrónico, donde se incluirá dicha información, las finalidades para las que supuestamente ha dado su aprobación (incluido el envío de comunicaciones comerciales) y dándole la opción de la revocación de alguna de ellas.

- **No enviar documentación por fax.**

  Al no existir modo de garantizar que la persona que recibe el fax, conteniendo datos de carácter personal, es realmente el interesado, este medio de comunicación no es el adecuando.

  Por lo tanto, se deberá evitar su utilización en la medida de lo posible.

- **No dar información a nadie que no sea el interesado o su representante legal**

  La ley prohíbe comunicar datos de carácter personal de una persona a otra que no sea él mismo o su representante legal (debidamente acreditado).

  Por lo tanto, salvo que previamente haya sido autorizado por el interesado, no se podrá entregar documentación o informar a personas no autorizadas, aunque sean familiares.

  En el caso de que alguien, en su nombre, solicite alguna información, se deberá poner en conocimiento del interesado y solicitar su autorización.

  Otra forma podrá ser la del envío de la información solicitada al propio interesado, para que sea él, bajo su propia responsabilidad, la que se la entregue a quien considere.

  En el caso de menores de edad la información solo se entregará a su(s) representante(s) legal(es).

- **Destruir de forma segura todos los documentos, estén en el soporte que estén, que contengan datos de carácter personal.**

  Todo documento que contenga datos de carácter personal debe se destruido garantizando que nadie va a poder acceder a su contenido, una vez haya dejado de ser necesario y hayan transcurrido los plazos legales.

  Por lo tanto, el uso de destructoras de papel es obligatorio (aunque para ello hubiera que desplazarse a otra área de la Empresa).

  También es necesario ser consciente de que los CD o DVD utilizados para hacer copias, deberán ser destruidos, cuando finalice su vida, de forma segura (a ser posible mediante destructoras), para garantizar que no se pueda acceder a todo o parte de su contenido.

  En el caso de archivos informáticos, la simple instrucción de borrado, a nivel informático, y el “vaciado de la papelera de reciclaje”, no son suficiente para que la información desaparezca.

Incluso, el formateo (rápido) de un disco tampoco llega a borrar, realmente, el contenido del mismo.

La única forma posible de destrucción segura es la de realizar un formatea “a bajo nivel” (lento), o la utilización de un software específico a tal efecto.

- **No realizar copias de documentos sin autorización del Responsable de Seguridad.**

  Cualquier reproducción de documentos, conteniendo datos de carácter personal debe ser autorizada por el Responsable de Seguridad.

- **Ante la duda, ser prudentes y consultar al Responsable de Seguridad.**

  Dado que en el trabajo diario pueden surgir infinidad de casos, recomendamos ser prudentes y consultar al Responsable de Seguridad.

2.5.- FUNCIONES ESPECIFICAS DEL PERSONAL DE SISTEMAS

Si el usuario, además de sus funciones, tiene privilegios para la administración de equipos informáticos, deberá conocer las obligaciones que le corresponden como personal informático.

Debido al especial acceso que tiene el personal informático se le atribuyen unas responsabilidades complementarias:

1) Guardar secreto de toda la información de carácter personal, o que afecte a ésta, de la que tenga conocimiento en el desarrollo de su de trabajo, aún después de acabada la relación con la organización.

2) Aunque debido a sus funciones disponga de un acceso privilegiado a ciertos recueros, se compromete a acceder únicamente a los datos necesarios para desarrollar sus funciones.

3) En el caso que detecten, deficiencias de seguridad en el sistema de información, lo deberán comunicar al Responsable de Seguridad correspondiente.

4) Colaborar con el Responsable/s de Seguridad en la resolución de las incidencias que se le encarguen.

5) Desempeñar sus funciones con estricta observancia de las obligaciones dispuestas por la legislación sobre protección de datos.

3.- PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS

El Responsable de Seguridad habilitará un Libro de Incidencias, con el fin de que se registren en él, cualquier incidencia relacionada con datos de carácter personal, y que puedan o no suponer un peligro para la seguridad de los mismos.

El Responsable de Seguridad analizará las incidencias registradas, y tomará las medidas oportunas, tanto para solucionarlas como para evitar que se vuelvan a producir.

Según figura en el apartado de Funciones y Obligaciones del personal, cualquier usuario que tenga conocimiento de una incidencia es responsable de su comunicación al Responsable de forma inmediata.

En el caso de que la incidencia haya producido la pérdida de datos en ficheros de nivel medio, para ejecutar los procedimientos de recuperación, será necesaria la autorización por expresa del Responsable del Fichero.

En el momento que, cualquier usuario (propio o externo) detecte cualquier incidencia, seguirá el procedimiento siguiente:

- El usuario que tenga conocimiento de la incidencia se responsabiliza directa y personalmente de registrarla en el impreso habilitado a tal efecto, entregándolo a continuación y sin demora al Responsable del departamento para su comprobación y validación, quien, también de forma inmediata, lo pondrá en conocimiento del Responsable de Seguridad.

- El Responsable de Seguridad tomará de inmediato las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la incidencia.

- Una vez subsanada, el Responsable de Seguridad analizará las posibles causas por las que se haya podido producir la incidencia, con el fin de tomar las medidas correctoras adecuadas con el fin de que no se vuelva a repetir.

- En el caso de que se hayan visto afectados ficheros con datos de nivel medio o alto y sea necesario llevar a cabo algún procedimiento de recuperación de datos, será imprescindible que el Responsable del Fichero autorice la ejecución del citado procedimiento, haciéndolo constar mediante su firma en el impreso de registro de incidencias.

- No registrar una incidencia de la que se haya tenido conocimiento, o no entregar el impreso cumplimentado al Responsable, será considerado una falta contra la que se podrán imponer sanciones

NOTIFICACIÓN DE INCIDENCIAS	**Fecha**	
	Hora	
Persona que notifica		
Tipo de Incidencia		
Descripción detallada		
Efectos que ha producido		
Persona que realiza Comunicación	**Firma**	

Tendrá la consideración de incidencia respecto a los sistemas de información las siguientes:

- Pérdida de Información.
- Modificaciones y accesos no autorizados a los datos.
- La no revisión o modificación del Documento de Seguridad cuando ello fuera preciso.
- El desconocimiento de cualquier persona que trabaje en la empresa de las medidas de seguridad que le sean exigibles, según las funciones que tenga asignadas.
- La falta de notificación o de inscripción de incidencias.
- La inexistencia de relación actualizada de los usuarios de los sistemas de información.
- El incumplimiento de los procedimientos previstos para la autenticación.
- El incumplimiento de las medidas establecidas para la asignación, distribución y almacenamiento de contraseñas.
- El almacenamiento de forma inteligible de contraseñas.
- El acceso no autorizado a datos o recursos.
- El acceso a datos o recursos fuera de los horarios laborables.
- La falta de ejecución de los mecanismos que impidan al usuario el acceso a datos no autorizados.
- La modificación no autorizada de datos.
- El borrado no autorizado de datos.
- La salida no autorizada de soportes informáticos.
- El almacenaje de soportes informáticos que contengan datos en lugares de acceso público.
- La no realización de las copias de respaldo preceptivas en el tiempo que se fija en el presente Documento.
- El incumplimiento de las medidas establecidas para el desecho o reutilización de los soportes.
- El incumplimiento de las medidas de seguridad que persiguen salvaguardar la recuperación indebida de la información que se contenga en los soportes.
- La falta de autorización por escrito del responsable del fichero, para poder ejecutar la recuperación de los datos.
- La distribución en soportes, o transmisión por redes de telecomunicación, de información legible o susceptible de ser manipulada.
- El acceso por personal no autorizado a la sala de servidores.

4.- PROCEDIMIENTO DE ATENCIÓN DE DERECHOS DEL INTERESADO

La empresa debe en todo momento asegurar los derechos que los afectados tienen respecto a sus datos personales.

En el momento de que cualquier usuario tenga noticia de una solicitud de derechos por parte de un afectado, se lo comunicará de forma inmediata al Responsable de Seguridad.

Una vez recabada toda la información, por parte del Responsable de Seguridad, se la comunicará al Responsable del Fichero con el fin de que éste pueda resolverla en los plazos previstos en la ley.

Reclamación del afectado

Los afectados podrán realizar su reclamación de derechos de cualquier forma, siempre y cuando su solicitud reúna los requisitos mínimos:

- Derecho que reclama.
- Identificación. Deberá estar perfectamente identificado adjuntando fotocopia del DNI.
- Identificación del Representante. En caso de que la solicitud la realice un representante del afectado, éste deberá estar perfectamente identificado, aportando tanto su DNI , como el documento que le acredite como representante.
- En el caso de que la solicitud sea de modificación de datos, deberá adjuntar documentos que acrediten tales cambios.

Con este fin, se dispone de una serie de documentos, que en el caso de que la solicitud se realice en las propias oficinas de la empresa deberán ser utilizados.

En el caso de que la solicitud presente algún defecto, el Responsable del Fichero, está obligado a solicitar la subsanación del mismo al afectado, ya que si no lo hiciera la solicitud deberá ser denegada.

La solicitud de derechos, por parte del afectado debe ser mediante métodos gratuitos para el afectado, o por lo menos que no suponga ningún beneficio para la empresa

Comunicación al afectado

La comunicación al afectado deberá realizarse de la manera más segura posible, debido al contenido de la información, por lo que se utilizará, en cada caso, el método más adecuado que lo garantice.

En el caso de denegación de las solicitudes, se deberá comunicar al afectado los motivos.

El Responsable del Fichero, contestará a la solicitud, tanto si en el fichero figuran datos del afectado como si no figura ninguno.

En el caso de una solicitud de Derecho de Acceso, al afectado se le podrá ofrecer uno de los siguientes sistemas de consulta:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitido por correo.
- Fax.

5.- IMPRESO SOLICITUD DE AUTORIZACIONES

MODELO - IMPRESO DE AUTORIZACIÓN

Este impreso se utilizarán para realizar solicitudes de:

- Salida ordenadores portátiles con datos personales
- Tratamiento de datos fuera de los locales de la empresa.
- Creación de Ficheros Temporales.
- Pruebas con Datos Reales.

<table>
<tr><td colspan="3">SOLICITUD DE AUTORIZACIÓN</td><td>N.º</td><td></td></tr>
<tr><td>Tipo Solicitud</td><td colspan="2"></td><td>Fecha</td><td></td></tr>
<tr><td rowspan="2">Tipo Autorización</td><td>Periódica</td><td>Ordinaria</td><td colspan="2">Extraordinaria</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td>Motivo de Solicitud</td><td colspan="4"></td></tr>
<tr><td>Persona que solicita</td><td colspan="4"></td></tr>
<tr><td>Observaciones</td><td colspan="2"></td><td colspan="2">Firma Responsable Seguridad</td></tr>
</table>

6.- CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente Manual de Usuario, por parte del personal infractor, podrá ser considerado, dependiendo de las consecuencias que ello acarree al Responsable del Ficheros, como falta muy grave.

Las sanciones e indemnizaciones que le pudieran ser impuestas a la empresa, como consecuencia del incumplimiento, deliberado o negligente, por parte de un usuario de cualquier medida, norma, procedimiento, regla u obligación establecida en el presente manual serán repetidas por parte de la empresa contra el usuario infractor.

También se advierte que, en cualquier caso, los afectados titulares de los datos de carácter personal pueden dirigir sus acciones civiles, e incluso penales, directamente contra el infractor causante del daño, con independencia de su condición de responsable de los ficheros o simple usuario.