

GUIA DE PROTECCIÓN DE DATOS PARA PERSONAL
CON ACCESO A LA INFORMACIÓN DE CARÁCTER
PERSONAL CONTENIDA EN LOS SISTEMAS DE

**ASOCIACIÓN NOESSO
(NO ESTÁS SÓLO)**

NOVIEMBRE 2010

INDICE

Introducción	1
Ámbito de Aplicación	2
Conceptos Básicos	3
Acceso y Comunicación de la Información contenida en los Sistemas de Información	5
Normas comunes para usuarios de los sistemas de información: 1. Usuarios autorizados 2. Obligaciones del personal. Consecuencias de su incumplimiento. 3. Identificación, autenticación 4. Acceso y conexión a puestos de trabajo 5. Gestión de incidencias 6. Gestión de soportes 7. Copias de Respaldo	6 6 7 9 12 13 15
Comunicación y control de la información: 1. Comunicación de la información 2. Control de la información 3. Tratamiento de Datos de Carácter Personal 4. Derechos de los titulares de los datos 5. Cesiones de datos a terceros	16 17 19 21 24
Anexo Legislativo	26

GUÍA DE PROTECCIÓN DE DATOS PARA EL PERSONAL

Introducción

La Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, su honor e intimidad personal y familiar.

Esta Ley ha sido desarrollada por el Real Decreto 1720/2007, por el que se aprueba el Reglamento de Protección de Datos de los Ficheros Automatizados de Datos de Carácter Personal. En este Reglamento se establecen las medidas de seguridad de índole técnica y organizativa necesarias a adoptar respecto de los ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas y, en general, todas las personas que intervengan en el tratamiento de datos de carácter personal.

Con la aparición de esta normativa y, la consecuente necesidad de adaptación y cumplimiento de la misma por todas aquellas entidades que lleven a cabo un tratamiento de datos personales, nuestra Organización, se ha planteado la necesidad de adaptar las medidas de seguridad implementadas en los ficheros con datos de carácter personal, en cumplimiento de la legislación vigente en la materia.

El conocimiento y cumplimiento de esta normativa vincula a todos los empleados integrantes de la asociación que intervengan, de forma directa o indirecta, en el tratamiento de datos de carácter personal en el ejercicio de sus funciones.

Por ello, para posibilitar el cumplimiento de esta normativa, se requerirá la colaboración necesaria del personal integrante de la asociación, puesto que, en el desarrollo y ejercicio de la actividad diaria, la mayor parte de los empleados y profesionales, de forma necesaria, maneja y trata datos personales. Piénsese en los datos de personas de contacto de entidades colaboradoras, proveedores, empleados, o personas aspirantes a un puesto de trabajo en nuestra Organización en un proceso de selección.

En este sentido, la asociación con objeto de velar y hacer cumplir la normativa de protección de datos, ha nombrado un "Responsable de Seguridad", el cual se encarga de coordinar, controlar, desarrollar y verificar el cumplimiento de las medidas, normativas y procedimientos mencionados en el Documento de Seguridad de la Compañía conforme a lo establecido en el Reglamento de Protección de Datos.

Ámbito de Aplicación

La presente Guía de Seguridad pretende establecer el procedimiento a seguir por el personal de la asociación que maneje datos de carácter personal, en el desarrollo de su actividad diaria, así como concienciar a los mismos de su importancia.

En este sentido se encuentra directamente dirigida a los siguientes destinatarios:

- Personal propio, puesto que para el desempeño de las actividades que le corresponden, necesariamente efectúan un tratamiento de datos de carácter personal. Piénsese en la gestión de clientes, gestión de facturas, gestión de llamadas, gestión de proveedores, contabilidad, etc.
- Personal externo, que presta servicios en las instalaciones de la Entidad y requiere el acceso a datos personales de titularidad de ésta, para lo cual necesariamente deberá conocer cada uno de los procedimientos de seguridad y manuales implantados en la misma.

A los efectos de la presente Guía, este personal enumerado anteriormente, así como cualquier otro que por razón de su puesto en la Organización efectúe un tratamiento de datos personales, será calificado como “los Usuarios” o “el personal”.

En consecuencia, la operativa general para el cumplimiento de la normativa de protección de datos por el personal de la Entidad que se describe a continuación, será aplicable a todas las actividades que se desarrollen e impliquen el manejo y tratamiento de datos personales, desarrolladas en cualquiera de las Unidades o Áreas que la componen, si bien, teniendo en cuenta las peculiaridades propias establecidas en determinados procedimientos específicos por razón de la materia.

Conceptos Básicos

A continuación, se definen algunos conceptos considerados básicos que ayudarán a determinar, en cada momento, el carácter de la información tratada. Esto es, si la información constituye un dato de carácter personal, si el archivo que recoge los datos personales se considera un fichero y si el uso que se hace del mismo constituye, a efectos de la Ley Orgánica de Protección de Datos, un tratamiento de datos de carácter personal.

a) Datos de carácter personal: Por dato de carácter personal se entiende, cualquier información concerniente a personas físicas identificadas o identificables.

La definición anterior de dato de carácter personal incluye todo tipo de información, ya sea numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión.

A continuación, con carácter ejemplificativo, se incluye un listado de datos de carácter personal:

- *Datos identificativos*: nombre y apellidos, dirección postal o electrónica, teléfono, DNI/NIF, nº SS/mutualidad, imagen o voz, firma o huella digitalizada, firma electrónica o marcas físicas, etc.
- *Datos de características personales*: estado civil, familia, fecha y lugar de nacimiento, edad, sexo, nacionalidad, lengua, características físicas, etc.
- *Datos de circunstancias sociales*: situación militar, propiedades, rentas, estilos de vida y aficiones, pertenencia a asociaciones, licencias, etc.
- *Datos académicos y profesionales*: formación, titulaciones, experiencia profesional, detalles de empleo, etc.
- *Datos especialmente protegidos*: ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Fichero: Se entiende por fichero, todo conjunto organizado de datos de carácter personal, con independencia de la forma o modalidad de su creación, almacenamiento, organización y acceso.

Para determinar los supuestos de existencia de un fichero no sólo se debe atender a si el mismo ha sido creado utilizando una herramienta informática específica para el almacenamiento de datos, como una base de datos tipo Access, Oracle, SQL, etc., sino que cualquier soporte que contenga datos de carácter personal de forma organizada, como una hoja de Excel o un documento Word, pueden ser calificados también como un "fichero", a efectos de lo establecido en la Ley Orgánica de Protección de Datos.

En todo caso, para que un fichero pueda calificarse como un fichero de datos personales, deberá contener algún dato de carácter identificativo de la persona.

c) Tratamiento de datos: Se entiende por tratamiento de datos, toda operación o procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como la cesión de datos a personas ajenas a la Organización o a otras empresas, incluso que formen parte de un mismo Grupo Empresarial, las cuales resulten de comunicaciones, consultas, interconexiones y transferencias.

La definición anterior de tratamiento de datos tiene un carácter amplio y abarca cualquier utilización de los datos personales realizada por el personal en la Entidad. Por tanto, se considera tratamiento de datos toda utilización realizada

por un empleado en el desarrollo de sus funciones en la Entidad, efectuado en cualquier momento de la "vida" del dato, esto es, desde la recogida hasta la cancelación o bloqueo de los datos.

Consecuencia de lo anterior es que cualquier uso u operación que se realice de datos de carácter personal por un empleado en el desarrollo de las actividades de la Entidad deberá ajustarse y respetar lo establecido en el presente Manual.

d) Incidencia: cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

Acceso y comunicación a la información contenida en sistemas de información

Se entiende por información contenida en sistemas de información, a efectos de las presentes normas, el conjunto de datos de carácter personal existentes en los ficheros de datos o en las distintas aplicaciones informáticas que el personal de la asociación utiliza para el desarrollo de su actividad profesional o para el desempeño de su función o cargo.

El acceso a esta información sólo está permitido a usuarios autorizados, para la realización de las funciones propias de la gestión, encaminadas al cumplimiento legítimo de la finalidad antes dicha para que estos ficheros han sido creados, sin que la información obtenida pueda ser cedida a terceros, salvo en los casos expresamente permitidos por la Ley o por la norma reguladora de creación del fichero.

Normas comunes para los usuarios de los sistemas de información

1.- Usuarios autorizados

El Responsable de seguridad designará a las personas con acceso autorizado a los locales, sistemas y ficheros protegidos para su tratamiento.

Los referidos usuarios autorizados solamente podrán acceder a los ficheros para los que han sido autorizados.

2.- Obligaciones del personal. Consecuencias de su incumplimiento

El personal guardará absoluta confidencialidad y deber de secreto sobre los datos de los ficheros y en ningún caso dará un tratamiento conducente al logro de una finalidad distinta o incompatible para la cual ha sido creado el fichero.

Asimismo, son de obligado cumplimiento todas normas descritas en el Documento de seguridad y en la presente Guía de Seguridad para el personal del mismo, por lo que todos los empleados firmarán una carta de confidencialidad y de responsabilidad frente al uso indebido de los datos y a la obligación de deber de secreto que estipula la legislación vigente ante los datos de carácter personal, en conformidad a su entendimiento de las normas de seguridad antes dichas, la cual se archivará conjuntamente con el Documento de seguridad del despacho o en el expediente personal de cada usuario.

Se deberá comunicar cualquier incidencia que surja en el tratamiento de los datos y pueda afectar a su seguridad al RESPONSABLE DE SEGURIDAD, en el plazo máximo de veinticuatro horas de haberse detectado.

El personal que incumpla con alguna de la normativa vigente en materia de protección de datos, correrá con las consecuencias que se detallan en el ANEXO LEGISLATIVO que se acompaña, aparte de las repercusiones de carácter laboral en que pudiera incurrir.

3.- Identificación y autenticación

Todos los Usuarios de los sistemas de información utilizados en la asociación dispondrán de contraseñas asociadas a sus identificadores de usuario para permitirles el acceso a los sistemas informáticos (login y password), los cuales tendrán la consideración de personal e intransferible. Cada Usuario sólo tendrá acceso a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones dentro de la asociación.

Es obligatorio por parte del Usuario, en su primer acceso al sistema o a una aplicación, el cambio de la contraseña asignada al ser dado de alta o en el procedimiento de asignación por olvido de la contraseña, en cuyo caso deberá ponerse en contacto con el Administrador del Sistema quien le advertirá de esta circunstancia.

Se establecerá un sistema de seguridad informática, que garantizará que sólo pueda acceder a los ficheros el personal autorizado, para identificar y autorizar el acceso a los sistemas de información automatizados en dos niveles:

Un "Login" para que los USUARIOS AUTORIZADOS puedan desde su ordenador acceder a los recursos informáticos que gestionan los ficheros.

Un "Password" para el acceso a los programas y/o ficheros para los que están autorizados.

A cada usuario deberá asignársele un "Login" y un "password" asociado. El primero servirá para identificar al usuario cuando acceda al sistema de

información y el segundo permitirá la autenticación del mismo ante el sistema, los cuales quedarán registrados de forma cifrada e ininteligible.

El "Login" será único en todo el sistema y estará formado por una cadena de caracteres que en el caso de las personas físicas será una abreviatura de su nombre y apellidos.

El "password", o contraseña, se asignará a cada usuario por el Responsable de Seguridad o será elegido por cada usuario y está formado por una combinación de letras y/o números con una longitud mínima recomendable de 4 caracteres, debiendo consistir en un conjunto de caracteres alfabéticos y alfanuméricos, combinando caracteres en mayúscula y minúscula y/o utilizando signos de puntuación, en cuanto se posibilite por el sistema y/o aplicación.

La contraseña no será fácilmente deducible. Para ello, se recomienda no seleccionar como contraseña palabras en cualquier idioma o códigos de valores asociables al usuario (nombres de personas, matrículas, teléfonos, fechas, etc.), permutaciones sencillas o secuencias de teclado, ni utilizar en los cambios de contraseñas secuencias lógicas fácilmente deducibles.

El cambio de la contraseña se efectuará con una periodicidad mínima de una vez cada SEIS MESES.

La contraseña variará con cada renovación, no permitiéndose la práctica de mantener un juego de contraseñas utilizándolas de forma cíclica.

El sistema de seguridad sólo permitirá la recuperación de las contraseñas al RESPONSABLE DE SEGURIDAD, siendo el usuario el único responsable de su memorización. En el caso de olvido será necesario solicitar al Responsable de Seguridad una contraseña nueva inmediatamente que sustituirá a la anterior.

El sistema bloqueará el acceso de un usuario cuando se introduzca la contraseña erróneamente durante 3 intentos. El bloqueo consistirá, atendiendo a la naturaleza de los datos a los que se pretenda acceder, en salir sin ejecutar (nivel básico) o en bloquear la estación de trabajo (nivel medio-alto), pudiendo ser desbloqueada la máquina exclusivamente por el responsable de seguridad. En todo caso, se registrará el intento de acceso no autorizado por el sistema de seguridad. Este tipo de situación puede ser objeto de auditoria por parte del sistema.

Si el Usuario conserva escritas las contraseñas, deberá mantenerse en lugares no accesibles a terceros, evitando su colocación en lugares visibles y cercanos al puesto de trabajo (como el caso de anotaciones en el ordenador, en la mesa de trabajo, etc.).

Cada usuario será responsable de las consultas y modificaciones que se efectúen sobre los distintos sistemas de información con su login de usuario y password, por lo que deberá poner especial atención en la elección de ésta y en el

mantenimiento de su confidencialidad, negando el acceso al sistema a otras personas con su login de usuario y password. El usuario no podrá ceder su login y password a terceros.

Para posibilitar la confidencialidad de las contraseñas se requerirá la colaboración de los Usuarios. En este sentido, se encuentra expresamente prohibida la divulgación o comunicación por los Usuarios de su clave de acceso a otras personas integrantes de la plantilla o ajenas a la Entidad. Por tanto, cada Usuario es responsable de la confidencialidad de su contraseña y de todas las actividades realizadas sobre el sistema con su identificativo de usuario a los sistemas de la Organización.

En caso de que el identificador de usuario o clave de acceso fuera conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicar esta incidencia inmediatamente, poniéndolo en conocimiento del "Responsable de Seguridad" y del Administrador del Sistema para proceder a su cambio.

4.- Acceso y conexión a los equipos y puestos de trabajo

Los empleados de la asociación deberán respetar las estipulaciones y normas vigentes establecidas para el correcto tratamiento, uso y manipulación del material de trabajo que se pone a disposición del Usuario.

El uso de los recursos y del material puesto a disposición por la Entidad deberá orientarse al cumplimiento de las finalidades previstas para la ejecución de las funciones encomendadas a los empleados. Por tanto, no se posibilita la utilización de los recursos de la misma por los empleados con fines personales o ajenos a los objetivos propios del puesto de trabajo correspondiente.

En el caso de la existencia de grabadores de CD`s en la Entidad, los Usuarios deberán tener en cuenta que no se posibilita un uso personal de los mismos, por lo que no se podrá grabar y almacenar información en los mismos con fines personales, debiendo evitar la posible salida incontrolada de información de las instalaciones de la Organización.

No obstante, en supuestos en que por motivos justificados de trabajo se requiera la salida de este tipo de soportes de las instalaciones de la Entidad, se deberá comunicar esta circunstancia al "Responsable de Seguridad" de la Entidad.

El acceso de un usuario está restringido a los equipos físicos (terminales, PCs, etc.) de acceso al sistema que le asigne el responsable de seguridad.

La conexión de los equipos físicos está restringida a puntos concretos de acceso a la red de comunicaciones.

En caso de ausencia, aunque sea momentánea, del puesto de trabajo, el usuario deberá dejar las aplicaciones que contengan datos personales cerradas, mediante la salida de las mismas, de manera que no se permita la visualización de datos por personal no autorizado (por ejemplo, mediante un protector de pantalla; la reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente).

Al finalizar su turno de trabajo, cada Usuario será responsable de apagar su equipo, ya que si el equipo quedara encendido y algún fichero de la red abierto, el proceso de back-up no comprenderá ese archivo por lo que no se realizará la correspondiente copia de seguridad del mismo.

En el caso de Uso de Impresoras, el usuario deberá asegurarse de que no quedan documentos en la bandeja de salida que contengan datos protegidos. En caso de impresoras compartidas con otros usuarios, los usuarios deberán retirar los documentos conforme vayan siendo impresos. Igual procedimiento debe utilizarse para el caso de utilización de fax o scanner.

Los ordenadores portátiles se deberán mantener siempre controlados, evitando su posible sustracción. Respecto de los mismos, el Usuario deberá eliminar toda la información que no vaya a ser utilizada, la cual deberá volcarse en una Carpeta de Red, en la que se encuentren implantadas las medidas de seguridad correspondientes, conforme le sea indicado por el "Responsable de Seguridad".

El envío electrónico de información y la utilización de Internet por parte de los empleados de la Entidad se encuentra exclusivamente permitida en relación con el desempeño de las actividades laborales que corresponden a cada empleado, no encontrándose permitido su uso para finalidades distintas a las mencionadas anteriormente.

El puesto de trabajo sólo dispone de las conexiones imprescindibles y autorizadas para el acceso al sistema de información y a las distintas aplicaciones informáticas corporativas, que normalmente consiste en una conexión a la red de comunicaciones.

No se permite la conexión externa o interna al puesto de trabajo de dispositivos de almacenamiento, de comunicaciones o de cualquier clase que no hayan sido previamente autorizados por el Responsable de seguridad. En particular existe un registro con los puestos que tienen conectados modems o cualquier equipo de comunicaciones y equipos de almacenamiento externos (unidades zip, disqueteras, etc.).

En ningún caso se permite la apertura y/o manipulación de los equipos informáticos y de comunicaciones por personal no autorizado.

5.- Gestión de Incidencias

Se entiende por incidencia cualquier anomalía que pudiera producirse y suponer un peligro para la seguridad de los ficheros de datos de carácter personal, entendida en sus vertientes de confidencialidad, integridad y disponibilidad de los datos.

Los Usuarios deberán tener en cuenta, entre otras, las siguientes incidencias:

1. La caída del sistema de la seguridad informática, por cualquier causa, que posibilite el acceso a los datos personales por personas no autorizadas.
2. El intento no autorizado de salida de un soporte.
3. La destrucción total o parcial del soporte físico en el que se encuentren datos personales.
4. El cambio de ubicación física de ficheros de datos personales.
5. Los intentos de acceso no autorizados o fallidos a ficheros con datos de carácter personal.
6. Conocimiento por terceros del identificador de usuario o clave de acceso al sistema.
7. Modificación de datos por personal no autorizado o desconocido.
8. Pérdida de información.
9. Existencia de sistemas de información sin las debidas medidas de seguridad.

Ante el acaecimiento de una incidencia, el Usuario deberá observar las siguientes normas:

1. Los Usuarios que tengan conocimiento de una incidencia deberán comunicarla inmediatamente como incidencia de seguridad, al "Responsable de Seguridad", el cual quedará encargado de la gestión y resolución de la misma.
2. El "Responsable de Seguridad" recibirá las notificaciones de incidencias y procederá a su registro, comunicándolas, a su vez, a los técnicos internos o externos encargados de la seguridad del sistema.
3. El conocimiento y la no notificación de una incidencia por parte de un Usuario será considerado como una falta contra la seguridad de los ficheros de la Organización.

6.- Gestión de Soportes

Soporte Informático: Se entiende por soporte informático todo objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se puedan grabar o recuperar datos, tales como cintas, cartuchos, CD-ROM o disquetes.

Identificación de Soportes: Los soportes que contengan ficheros de datos de carácter personal se identificarán, adecuadamente, con una etiqueta externa que la que se indique:

- De qué fichero se trata.
- Qué tipo de datos contiene.
- Proceso por el que se han originado.
- La fecha de creación del mismo.
- Carácter confidencial de la información.

Almacenamiento de Soportes: Los soportes se deberán almacenar en lugares a los que únicamente tengan acceso las personas autorizadas para el uso de los datos que contengan. Como medida general, se evitarán los cajones sin llave de cierre, superficie de mesas de trabajo y, en general, lugares accesibles o manipulables por terceros. Por otra parte, no se permite la existencia de soportes fuera de los lugares previstos para su custodia cuando no sean utilizados.

Funciones que permiten la copia de información en soporte electrónico:

- Por necesidades justificadas de trabajo
- Necesidad de proporcionar los datos a una empresa prestadora de servicios. En este caso, será requisito previo, la existencia de un Contrato que habilite dicha salida de datos.
- Realizar una captura de información para un determinado Proyecto, debidamente aprobado por una persona autorizada.

Destrucción de Soportes: Los soportes que vayan a ser retirados, destruidos o reutilizados deberán ser borrados, de forma que se impida la recuperación posterior de la información en ellos almacenada. Este mismo deber de destrucción será aplicable para la información contenida en formato papel.

Salida de Soportes: La salida de soportes con datos personales de las instalaciones, únicamente, se permitirá en supuestos justificados por necesidades de trabajo o bien para su comunicación a otras empresas o entidades cuando las circunstancias lo requieran. Esta circunstancia deberá ser comunicada al "Responsable de Seguridad", quien deberá autorizar dicha salida.

Sin perjuicio de lo anterior, toda entrada y salida de soportes deberá ser comunicada y autorizada por el "Responsable de Seguridad", quien informará al Usuario de las prevenciones que deberá adoptar en relación con el soporte, siguiendo el procedimiento establecido para la gestión de soportes.

Datos Especialmente Protegidos: En el supuesto de que se procediera a dar salida de soportes que incluyeran datos de carácter personal especialmente sensibles (referidos a ideología, religión, creencias, origen racial, salud o vida sexual) sería necesario proceder al cifrado de dichos datos. La salida de este tipo de soportes únicamente se efectuará previa petición al "Responsable de Seguridad".

7.- Copias de Respaldo

Los empleados deberán almacenar en el Directorio de Red correspondiente toda la información tratada en el desarrollo de sus funciones, lo cual permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se sometan a los procedimientos de copias de respaldo realizados en la Entidad.

Sólo en casos excepcionales, debidamente justificados y autorizados por el "Responsable de Seguridad", podrá el Usuario almacenar información en el disco duro de su ordenador, tanto en el PC como en el ordenador portátil. En este caso, se deberán realizar copias de seguridad de la información que el Usuario haya guardado, semanalmente, salvo que en ese periodo no se hubiera producido ninguna actualización de los datos. No obstante, una vez desaparecido el motivo que justificó el almacenamiento de información en una unidad local, se eliminará del disco duro y se volcará en la Carpeta de Red correspondiente.

Una vez establecidas las obligaciones que corresponden a todo el personal de la Entidad que, en el desempeño de sus actividades, lleve a cabo un tratamiento de datos de carácter personal, para finalizar, sería necesario recordar que, junto con el cumplimiento del presente Manual, este personal se encuentra sometido a las disposiciones y procedimientos recogidos en el "Documento de Seguridad" de la Entidad.

Comunicación y control de la información

1.- Comunicación de la información

No se podrá facilitar información contenida en los sistemas a terceros, por ningún medio o soporte, salvo en los casos y requisitos siguientes:

1.1 Comunicación de datos mediante personación en la asociación:

Se requerirá al interesado para su identificación el DNI, pasaporte o carné de conducir en caso necesario.

En caso de personas jurídicas, además de la identificación del representante se le exigirá el documento que le autorice para la actuación concreta (normalmente escritura de poder de representación).

En ningún caso se facilitará datos de carácter personal a persona distinta al titular de la información solicitada o al responsable del fichero, salvo autorización expresa y por escrito de algunos de éstos.

1.2 Información telefónica:

No se facilitará telefónicamente información de carácter personal si no se posee la absoluta certeza de que el solicitante es el titular de la información solicitada. Si mantenemos la más mínima duda sobre la identidad del solicitante, aunque el solicitante manifieste ser el propio titular o interesado, la naturaleza confidencial de esta información obligará a indicarle cuando proceda, que por su propia seguridad y en cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal no se facilitará la información por teléfono, si bien se podrá remitir al domicilio que consta en la base de datos o en caso de requerimiento urgente se le invitará a desplazarse al Despacho Profesional, comunicando esta circunstancia al Responsable de Seguridad de la asociación.

La información a facilitar por teléfono sólo puede estar relacionada con asuntos generales de materia laboral, fiscal, contable o mercantil, no pudiendo facilitar telefónicamente ningún dato calificado por la LOPD como especialmente protegido tales como datos de salud, religión, creencias, ideología, origen racial, vida sexual, afiliación sindical, minusvalías ...

1.3 Otros medios:

En ningún caso se facilitará información a través de cualquier otro medio de comunicación no contemplado en estas normas, sin la autorización del Responsable de Seguridad, con la excepción del telefax, cuando así haya sido solicitado por el interesado o lo aconseje la urgencia de la comunicación y siempre que el receptor del mismo tenga implantadas las medidas de seguridad de protección de datos vigentes.

2.- Control de la información

No se podrán hacer consultas o modificaciones a los ficheros informáticos que no estén relacionadas con las competencias propias del usuario.

Todo usuario deberá mantener absoluta discreción y confidencialidad sobre los datos directamente contenidos en soportes informáticos, listados u otro material que contenga información de carácter personal, así como la contenida en los expedientes administrativos.

Los documentos que contengan datos de carácter personal tales como impresiones de pantalla, listados, pruebas de impresión o ficheros temporales o variables, que no deban conservarse en el expediente, deberán ser destruidos una vez que haya dejado de ser necesario para los fines que motivaron su creación. Tal destrucción se hará de forma que impida su reconstrucción. En todo caso deberá hacerse un uso restrictivo de las impresiones de pantalla.

Solamente los usuarios autorizados por el responsable del fichero o por el encargado de su tratamiento, tendrá acceso físico a los locales donde se encuentran ubicados los sistemas de información y/o los archivos físicos con datos de carácter personal.

Queda prohibido sacar fuera de las instalaciones de la asociación documentos o ficheros informáticos, ya sea en soporte papel ya sea en cualquier otro tipo de soporte informático susceptible de recuperación de datos, salvo que medie expresa autorización del responsable del fichero, existiendo un inventario de soportes y un registro de entradas y salidas de los mismos a cargo del responsable de seguridad, sujetas a la normativa expuesta en el Documento de Seguridad.

La ejecución del tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable de seguridad.

Todos los soportes que contengan información de carácter personal como diskettes, CD'S, streamer, discos duros ... y que vayan a ser destruidos por haberse quedado desactualizados, deberán ser inutilizados, previa autorización del responsable de seguridad, mediante formateo de dichos soportes dejándolos físicamente inoperativos y posteriormente se desechará por los conductos necesarios para su reciclaje, como mediante la entrega de estos soportes al vertedero de la ciudad. En ningún caso se podrá proceder a la destrucción de ficheros en soporte papel sin la previa autorización del responsable de seguridad, utilizando para su desintegración algún método que no permita reconstruir, ni siquiera parcialmente, la información de carácter personal, como, por ejemplo, mediante la utilización de destructoras de papel o incineración de los soportes documentales.

Todo usuario deberá conocer la legislación aplicable a la materia, un extracto de la cual se incluye como anexo. Una copia de la carta adjunta de confidencialidad, secreto y responsabilidad frente al uso indebido de los datos, una vez firmada por el usuario, se archivará en el expediente personal.

3.- Tratamiento de Datos de Carácter Personal

El Reglamento de Protección de Datos divide en tres niveles distintos los datos de carácter personal, dependiendo de la naturaleza de los mismos y de la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información:

Nivel Básico: datos de carácter meramente identificativo tales como nombre, apellidos, DNI, edad, dirección, teléfono...etc.

Nivel Medio: datos relativos a comisiones de infracciones administrativas o penales, Hacienda Pública, servicios financieros. A su vez, se entenderán por ficheros de nivel medio al conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

Nivel Alto: datos relativos a ideología, religión, creencias, origen racial, salud o vida sexual, datos recabados con fines policiales sin consentimiento de las personas afectadas.

La información concerniente a los titulares de los datos debe obtenerse de forma lícita. Lo anterior supone que no se podrán recabar datos personales sin contar con el previo consentimiento de los titulares de los datos, salvo en varias circunstancias, entre ellas:

- Que los datos procedan de fuentes accesibles al público (*por fuentes accesibles al público* se entiende, exclusivamente, las enumeradas en la Ley Orgánica de Protección de Datos: el censo promocional, los repertorios telefónicos, las listas de colegios profesionales, los Diarios y Boletines Oficiales y los medios de comunicación).
- Que los datos se refieran a las partes de una relación comercial, laboral o administrativa.
- Que el tratamiento de los datos sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto en el que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Los datos considerados especialmente protegidos (*datos referentes a: ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual*) se encuentran sometidos a un régimen más estricto: se requiere, en unos casos, el consentimiento expreso, y en otros, el consentimiento expreso y por escrito del interesado para recabar este tipo de datos. En estos casos, cuando se pretenda la recogida de este tipo de datos se deberá comunicar esta circunstancia al "Responsable de Seguridad".

Igualmente, conviene señalar la necesidad de modificación y actualización de los ficheros con datos de carácter personal, siendo consecuencia del deber de

exactitud de los datos establecido en la normativa de protección de datos, lo cual supone que los datos deberán ser exactos y puestos al día de forma que respondan con veracidad a la **situación actual del afectado**. En aplicación de este principio, los datos que figuren en los ficheros de la Entidad han de adecuarse y responder a la situación actual del afectado, deben estar actualizados y ser acordes con la realidad, de ahí la necesidad de colaboración por parte de todo el personal de la Organización.

De lo anterior se desprende, que resulta de vital importancia la **exactitud de los datos personales** contenidos en los ficheros, puesto que no tenerlos actualizados supone la comisión de una infracción tipificada en la normativa de protección de datos.

Por otra parte, los empleados deberán considerar, que la totalidad de la información que gestionen, en el desempeño de sus funciones, es de **propiedad exclusiva** de los afectados, esto es, de las personas titulares de los datos personales, y los ficheros en los que se almacenan dichos datos, de la Entidad, por lo que no podrán disponer de ella para fines personales o cualquier otro no compatible con el fin que cumpla el fichero en el que se encuentran los datos.

Por último, los datos no serán conservados en forma en que se permita la identificación del afectado durante un periodo superior al necesario para los fines respecto de los cuales hubieran sido registrados. Una vez haya desaparecido la finalidad que justifica la creación del fichero, éste deberá ser bloqueado (si alguna ley exige su mantenimiento) o borrado, cumpliendo con el procedimiento establecido para estos supuestos en el presente documento.

4.- Derechos de los titulares de los datos

DERECHO DE INFORMACIÓN: Este derecho permite al afectado o interesado obtener, en el momento de recogida de sus datos personales, información relativa a la existencia de un fichero en el que los datos recabados son incorporados para su tratamiento automatizado por la Organización con un fin o finalidades determinadas.

Información cuando los datos son recabados del propio interesado: Se informará de modo expreso, preciso e inequívoco al interesado, previamente a la recogida de sus datos:

1. Existencia de un fichero donde se vayan a tratar los datos de carácter personal y finalidad del tratamiento.
2. Carácter obligatorio o facultativo de la respuesta a las cuestiones que se le planteen si los datos se recogen a través de un formulario o similar.
3. Consecuencias de la negativa a contestar alguno de los puntos incluidos en dicho formulario o preguntas que se planteen de forma verbal.
4. Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

5. Identidad y dirección de la empresa responsable del fichero o del tratamiento en su caso y lugar donde poder ejercitar sus derechos.
6. Existencia de cesión o comunicación de datos a terceros y la finalidad del tratamiento a realizar por éstos.

Si la recogida de datos se realiza de forma verbal y presencial, si se recogen de manera informatizada se realizará una impresión de los datos recogidos en la ficha en la que consten las menciones de información o bien se utilizará un modelo preimpreso. El cliente firmará el documento que será guardado por la Inmobiliaria.

Si los datos personales del cliente se recogen de forma telefónica, hay que informarle, brevemente, de todo lo anteriormente expresado en cuanto a los derechos de información y finalidad del tratamiento de los datos.

Información cuando los datos no han sido recabados del propio interesado: Si los datos de carácter personal no son recogidos directamente del interesado, este deberá ser informado de forma expresa, precisa e inequívoca por la asociación en los tres meses siguientes al registro de sus datos.

Se deberá informar del contenido del tratamiento, de la procedencia de los datos, de la finalidad, de los destinatarios de la información, de la posibilidad y forma de ejercitar los derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección de la Empresa responsable del fichero o del tratamiento donde poder ejercitar los derechos.

Tratamiento de datos personales en el ámbito de Internet: Cuando se realicen comunicaciones comerciales por vía electrónica éstas deberán identificarse claramente, identificar la persona jurídica en nombre de quien se realizan e incluirán al comienzo del mensaje la palabra PUBLICIDAD.

La Ley de Servicios de la Sociedad de la Información prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Esto no será de aplicación cuando exista una relación contractual previa, siempre que los datos se hayan obtenido de forma lícita y se empleen para el envío de comunicaciones comerciales referentes a productos o servicios de la propia asociación que sean similares a los que inicialmente fueron objeto de contratación.

Siempre la asociación deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales o publicitarios mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de datos como en cada comunicación comercial que realice.

DERECHO DE ACCESO: Este derecho permite al afectado o interesado solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos y las comunicaciones realizadas de los mismos por la Organización.

DERECHO DE RECTIFICACIÓN: Este derecho permite al afectado o interesado rectificar o corregir sus datos de carácter personal sometidos a tratamiento por la Organización, adecuándolos a la realidad existente.

DERECHO DE CANCELACIÓN: Este derecho permite al afectado o interesado solicitar la cancelación de sus datos personales sometidos a tratamiento por la Organización.

DERECHO DE OPOSICIÓN: Este derecho permite al afectado o interesado manifestarse negativamente, esto es, oponerse propiamente a un determinado tratamiento de sus datos realizado por la Organización.

Los titulares de los datos contenidos en los ficheros de titularidad de nuestra Entidad tienen reconocidos los derechos de acceso, rectificación, cancelación y oposición de sus datos.

Cualquier persona interesada incluida en estos ficheros tendrá derecho a solicitar y obtener, gratuitamente, información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevean realizar de los mismos a terceras entidades. Igualmente, se reconoce al interesado el derecho a rectificar o cancelar los datos personales que se hallen registrados en los ficheros de la Entidad, así como oponerse a un previo tratamiento de datos realizado por las mismas.

5.- Cesiones de Datos a Terceros

Cesión o comunicación de datos: Se entiende cualquier revelación de datos realizada a una persona distinta del interesado. Se considera cesión de datos toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por persona distinta de la afectada.

Cedente: Empresa o persona que lleva a cabo la comunicación de la información.

Cesionario: Empresa o persona que recibe la comunicación de la información.

Encargo de tratamiento: Se entiende por encargo de tratamiento, todo acceso efectuado por terceros a los datos, en el caso que nos ocupa, titularidad de la Entidad, cuando dicho acceso sea necesario para la prestación de un servicio a la misma.

Encargado del tratamiento: Empresa o persona física, autoridad pública o cualquier otro organismo que trate datos personales por cuenta del Responsable del Fichero, es decir, de la Entidad, en el caso que nos ocupa.

Es necesario que el personal de nuestra Entidad conozca y tenga en cuenta las siguientes consideraciones en la materia:

- Necesidad de la obtención del consentimiento del interesado para realizar cualquier comunicación de datos. En este sentido, el consentimiento se encuentra excepcionado en los siguientes supuestos:

- Por disposición de la ley o interés general
- Cuando se trate de datos obtenidos de una fuente accesible al público
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
- Por petición de la Administración de Justicia
- Cuando tenga por destinatarios al Defensor del Pueblo, Ministerio Fiscal, Jueces y Tribunales o el tribunal de Cuentas.

- La Agencia de Protección de Datos entiende que la comunicación de datos entre empresas de un mismo Grupo empresarial o bien entre entidades con una especial relación de colaboración se considera un supuesto de cesión de datos a terceros, por lo que se deberán cumplir los requisitos establecidos en la normativa de protección de datos.

En los supuestos en que sea necesario, en el desarrollo de la actividad, efectuar una cesión o comunicación de datos de carácter personal a una tercera entidad o bien, permitir un encargo de tratamiento por parte de terceros, los empleados de la Entidad implicados deberán tener en cuenta que:

- Se deberá comunicar previamente esta circunstancia al “Responsable de Seguridad” de la Entidad y esperar su autorización expresa para poder llevarla a cabo.

- En el caso de que se produzca un acceso de datos por parte de un tercero al objeto de prestar un servicio a la Entidad, será necesaria la adopción de un contrato por escrito que regule dicho acceso y la notificación de esta situación al “Responsable de Seguridad”.

ANEXO LEGISLATIVO

Código Penal

Artículo 197

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice sin perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en el apartado 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y sí se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 278

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 279

1. La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior.

Ley Orgánica de Protección de Datos de Carácter Personal (LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE). Resumen de Infracciones y Sanciones:

Infracciones Leves

- a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
- b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
- c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

Infracciones Graves

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el “Boletín Oficial del Estado” o diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

- j) La obstrucción al ejercicio de la función inspectora.
- k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
- l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

Infracciones Muy Graves:

- a) La recogida de datos en forma engañosa y fraudulenta.
- b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado, recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
- d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
- e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
- f) Tratar los datos de carácter personal de forma ilegítimo o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
- h) No atender de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal.

Sanciones:

Infracciones Leves: Multa de 601,01 a 60.101,21.- €

Infracciones Graves: Multa de 6.101,21 a 300.506,05.- €

Infracciones Muy Graves: Multa de 300.506,05 a 601.012,10.- €

Código Civil

Artículo 1.903

La obligación (de indemnizar) que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes de debe responder.

Los dueños o directores de un establecimiento o empresa (son responsables) respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones.

Artículo 1.904

El que paga el daño causado por sus dependientes puede repetir de éstos lo que hubiese satisfecho.