AYUNTAMIENTO DE GRANADA

CENTRO DE PROCESO DE DATOS
GABINETE DE SEGURIDAD
Expte.- 148/2012

DOCUMENTO MUNICIPAL DE SEGURIDAD

AYUNTAMIENTO DE GRANADA

DOCUMENTO MUNICIPAL DE SEGURIDAD (DS)

- EXPOSICIÓN DE MOTIVOS-

El vigente Documento Municipal (en adelante DS), fue aprobado por la Junta de Gobierno Local en sesión de 15 de Mayo de 2009. La versión que se somete a la aprobación de la Junta de Gobierno Local, pretende actualizar el documento tanto mediante la incorporación de las medidas y los procedimientos de Seguridad que deben regular los cambios operados en la organización y el funcionamiento de los servicios municipales y del Sistema de Información Municipal (en lo sucesivo, SIM), como con la adaptación de dichas medidas y procedimientos en aras de facilitar la futura implantación de la Administración Electrónica y del Esquema Nacional de Seguridad, y la rectificación de los errores sintácticos y de redacción detectados en la versión anterior, en aras de su concisión y mayor claridad. Siendo las modificaciones que se incorporan a la versión anterior, las siguientes:

- Modificaciones que se introducen en el Documento Municipal de Seguridad[1] -

Artículo 3.- Ámbito de aplicación.

El apdo. 1.c), de nueva redacción, incluye en el ámbito de aplicación del DS a las sociedades mercantiles de capital íntegramente municipal cuando ejerciten encomiendas de gestión, con base en el artículo 85.2 LRBRL, del se deduce que, en el ámbito de la Administración Electrónica, el DS deberá serles de aplicación. Habiéndose suprimido el anterior apdo. d), que hacía referencia asimismo a la aplicación del DS a las entidades y consorcios con participación mayoritaria del Ayuntamiento de Granada, cuando ejerciten potestades administrativas, toda vez que estas figuras no están incluidas en el ámbito de aplicación de la Ordenanza de Administración Electrónica, en consonancia con la misma.

Artículo 6.- Identificación y autenticación de usuarios.

Refunde los anteriores apdos. 1 y 2, estableciendo la identificación y autenticación del usuario y el alta previa en el mismo mediante el binomio usuario-contraseña, al objeto de evitar que el uso del núm. de usuario como identificador inicial, hasta ahora implantado, ocasione, por ser de fácil conocimiento general, problemas de accesos no autorizados. La refundición afecta al orden numérico de los restantes apartados del precepto.

El apdo. 3, de nueva redacción, regula el procedimiento de asignación de los rangos numéricos del personal de los recientemente absorbidos organismos autónomos, así como de las empresas y entidades públicas empresariales municipales que, aunque venían siendo adjudicados *de facto,* carecían de su reconocimiento *de iure*.

[1] No se mencionan, por su escasa importancia, las simples modificaciones de la redacción orientadas a la mejora del texto, ni las de concordancia por la introducción de nuevos artículos o a la supresión de otros.

El apdo. 7 suprime el número de caracteres exigido hasta ahora en la contraseña personal, ya que el mismo no se correspondía con la realidad, quedando con la siguiente redacción: *el modelo de contraseña adoptado es el de contraseña simple para acceso a los distintos componentes del SIM*.

Artículo 7.- Gestión de las autorizaciones de acceso.

El apdo. 5 de este artículo simplifica el anterior procedimiento de gestión de los recursos del SIM, igualmente regulado en el artículo 7 DS, introduciendo las siguientes novedades:

1. Desaparece la base de datos de Atención a Usuarios de Notes y el procedimiento de gestión de recursos gestionado con la misma, que exclusivamente podía iniciarse por las Jefaturas de Unidad mediante la formulación de las correspondientes peticiones escritas en aquella.

2. Se crea el Centro de Atención a Usuarios (C.A.U.), al que podrán comunicar directamente los propios usuarios la mayoría de sus necesidades, sin mediación de su Jefatura de Unidad, por vía telefónica (preferentemente) o por mensaje de correo electrónico o dirección web habilitada (en este procedimiento se incluyen las comunicaciones de averías, de incidencias generales, de renovación de recursos por caducidad, de incidencias de datos de carácter personal y de incidencias de los equipos). Quedando reservadas a las Jefaturas de Unidad únicamente las peticiones de acceso y cese de nuevos usuarios, las de recuperación de ficheros y las de dotación de recursos de hardware o de software no integrados en el equipo asignado.

Artículo 8.- Obligaciones de los usuarios del SIM.

A este precepto se han añadido 6 nuevos apartados, a saber:

1. Apdo.3, sobre la obligación de comunicar las averías, antes contenida en el artículo 7, pretende agrupar las obligaciones de los usuarios en el precepto adecuado.

2. Apdo. 4, que regula los procedimientos actualmente implantados de recuperación de información, incorporando la redacción del anterior artículo 16.3 DS, al que simplifica y sustituye.

3. Apdo. 5, sobre la regulación de la obligación de comunicar las incidencias de datos de carácter personal, que completa la del nuevo artículo 41 DS.

4. Apdos. 8 y 9, que concretan las obligaciones de los usuarios en cuanto a la adopción de algunas medidas de Seguridad Física y Lógica, por afectar a la protección de los equipos asignados y al tratamiento de la información que éstos contienen, que los convierte en responsables directos.

5. Apdo. 15, que regula el uso de las carpetas y ficheros de G-Unidad, y pretende tanto solventar los problemas de saturación de información en G:\Unidad, como arbitrar un

procedimiento para limitar, en su caso, el acceso a determinada información del personal regulado en el artículo 6.5 (personal becario o en prácticas).

6. Y apdo. 16 (escindido del anterior artículo 8.2.7 DS), que extiende la aplicación del régimen de disciplinario a la totalidad de las obligaciones de los usuarios reguladas en el precepto (lo que en la anterior no estaba suficientemente regulado), y deja patente la presunta responsabilidad de los usuarios tanto en los órdenes administrativo, civil, penal y ante la AEPD.

Artículo 10.- Tablón Electrónico.

De nueva inclusión en el DS, incorpora la regulación del Tablón Electrónico contenida tanto en el Decreto de Alcaldía de 27 de Julio de 2010, sobre la inserción de anuncios en el Tablón de Edictos de la Administración Electrónica Municipal, como en la Circular de la Delegación de Personal, Servicios Generales y Organización, de 9 de Septiembre de 2010, sobre el mismo asunto.

Artículo 11.- Tablón del Empleado.

Igualmente de nueva incorporación, completa la regulación del anterior artículo 10 DS, con las siguientes novedades:

1. Separa al correo electrónico del Tablón de Funcionarios.

2. Renombra el Tablón, que pasa de denominarse Tablón del Empleado, como viene siéndolo en la práctica.

3. Regula los contenidos de las cuatro secciones que lo componen.

4. Erradica prácticas no del todo acordes con la finalidad y el uso de esta base de datos, como son la inserción de anuncios publicitarios, de signo político (prohibidos por acuerdo plenario núm. 752 de 30/09/2011), y la publicación simultánea en varias de las secciones de anuncios con el mismo contenido.

Artículo 12.- Portal del Empleado.

De nueva inserción en el DS, regula la dualidad instrumental de esta base de datos, en cuanto medio para la inserción de los anuncios y contenidos del artículo 11.3.2 DS que se pongan a disposición de los empleados municipales en la Intranet, y como el sitio de la Sede Electrónica de la Administración Municipal para acceso restringido del personal municipal mediante Firma Electrónica tanto a los citados contenidos como a los del correo electrónico, la consulta de nóminas, la teleformación, el Tablón del Empleado, la gestión de permisos y licencias, el listín de teléfonos internos, las actas íntegras de las sesiones del Excmo. Ayuntamiento Pleno y el Callejero de Granada.

Artículo 13.- Uso del correo electrónico.

El apdo. 4 suprime la autorización de la Dirección General para anexar documentos al correo electrónico, toda vez que las versiones actuales del programa de comunicaciones internas (LotusNotes, v 8,5 o superiores) no permiten restricciones para los usuarios en el uso de anexos, lo que, aunque ha agilizado la transmisión de documentos, obliga a incrementar las medidas de prevención. A tal fin, se prohíbe la transmisión de datos de carácter personal por anexos fuera de dependencias municipales –ante el riesgo de su interceptación-, salvo que se cuente con la autorización expresa de la Dirección General para cada caso, con las excepciones que se indican (como la remisión de documentos a los boletines oficiales para su publicación).

Los apdos. 6 a 9 de la anterior redacción han sido suprimidos, por insertarse su contenido en otros preceptos del DS de más adecuada ubicación.

Artículo 14.- Acceso a datos de carácter personal en la atención personalizada de las oficinas municipales y transmisión por Internet, correo electrónico, soportes, vía telefónica o fax.

Se introduce este nuevo artículo a fin evitar posibles transgresiones del artículo 6 LOPD, derivadas tanto del uso de anexos de correo electrónico para la transmisión de datos de carácter personal como del hecho de que en los servicios se facilite información o se expidan recibos de impuestos municipales a personas distintas del titular, sin dejar constancia del consentimiento del mismo.

Artículo 15.- Centro de Proceso de Datos.

Incorpora una descripción de las áreas de división del CPD (incluida anteriormente en las definiciones de términos y conceptos del Anexo 1 DS). En el apdo. 3.1 se ha hecho referencia a las funciones de gestión de los dominios de servidores y a las de mantenimiento de todos los dominios.

Artículo 16.- Administradores.

En aplicación del artículo 10 del RD 3/2010, de 8 de Enero, por el que se regula el Esquena Nacional de Seguridad en el ámbito de la Administración Electrónica, que regula la seguridad como función diferenciada (información-servicio-seguridad), se incorpora en el apdo. 3 de este precepto la descripción de las distintas clases de Administradores generales del SIM y su adscripción orgánico-funcional, en el Centro de Proceso de Datos y en los restantes servicios municipales.

Artículo 20.- Procedimientos.

Modifica la redacción del anterior artículo 16.3 DS, suprimiendo parcialmente su redacción, así como al totalidad del 16.5, en concordancia con la nueva redacción dada al artículo 8.4 DS sobre recuperación de datos o ficheros.

Artículo 23.- Limitaciones de uso de hardware y software no normalizados.

En consonancia con la nueva regulación del artículo 7.5.b DS, la enmienda se fundamenta en la Circular del Tte. de Alcalde Delegado de Personal, Servicio Generales, de 8 de Marzo de 2012, sobre

tramitación de las peticiones de Hardware a través del CPD, condicionando la autorización de puertos USB, grabadoras y discos externos, a la obtención de autorizaciones de acceso en el Registro de Soportes, de manera que sólo los usuarios dados de alta en el mismo puedan utilizar aquellos, con lo que se incrementa el control de la información no autorizada que pudiera salir del SIM.

Artículo 24.- Registro de Soportes.

El enunciado del artículo, y la nueva redacción de su apdo. 2, se fundamentan en las mismas razones de la modificación anterior, que se dan por reproducidas.

Artículo 29.- Principios y deberes generales del tratamiento de datos de carácter personal: procedimiento de disociación de los datos; deber de confidencialidad; información y consentimiento de los afectados y publicación de datos de expedientes sancionadores.

Se modifica el apdo. 3, que transcribe el anterior artículo 32.3 DS, completándolo con la Instrucción de la Delegación de Personal, Servicios Generales y Organización, de 12 de Enero de 2011, sobre publicación de anuncios en la Web institucional y en el Tablón de Edictos Electrónico.

Se añade un nuevo párrafo al apdo. 8, con fundamento en la Resolución AEPD: R/00871/2010 / Procedimiento Nº AP/00094/2009, limitando la aplicación de los informes de aptitud relativos a los riesgos laborales, en el sentido de que los mismos serán comunicados a los empelados afectados y solo podrán ser conocidos por los mandos directamente vinculados con la atribución de funciones para su conocimiento y consideración a efectos de adaptación del puesto de trabajo.

Se añade asimismo el apdo. 10, que reproduce igualmente la citada Instrucción de la Delegación de Personal, Servicios Generales y Organización, de 12 de Enero de 2011, sobre publicación de anuncios de expedientes sancionadores.

El artículo refunde, suprimiéndolo, el anterior artículo 32 DS, por guardar éste mayor coherencia interna con el antiguo capítulo VII “Gestión de Datos de Carácter Personal”, al que ahora se le da la más correcta denominación de “Tratamiento de datos de carácter personal”, refundiéndose ambos capítulos en el nuevo capítulo VII, en aras de su simplificación.

Artículo 30.- Principios y deberes específicos del tratamiento de datos de carácter personal: adecuación, pertinencia, exactitud y finalidad de los datos.

El precepto transcribe el principio de *exactitud* del artículo 4.3 LOPD, que parece necesario recoger de forma expresa en el DS, en aras de evitar la tendencia -frecuente en la gestión administrativa- a no mantener debidamente actualizados los datos de carácter personal en los ficheros correspondientes.

Artículo 32.- Niveles de protección de los ficheros de datos de carácter personal.

Las modificaciones incorporadas al inciso final del apdo. 5 y al apdo. 6, se orientan a incrementar la seguridad jurídica, tanto mediante la concreción de las medidas de seguridad aplicables a

los ficheros de nivel Alto, reguladas de forma dispersa en el DS, como mediante la regulación –siquiera mínima– de la creciente puesta en producción de aplicaciones y programas que gestionan ficheros de este nivel de seguridad.

Artículo 40.- Procedimiento de tramitación de expedientes de cesión de datos de carácter personal.

Incorpora un nuevo apdo. 1, con el que se obliga a cumplimentar en cada entrega de cesión, previamente autorizada, de datos de carácter personal, una comparecencia o diligencia acreditativa de la resolución administrativa en que se fundamenta, la identidad del cesionario, el dato o datos cedidos y la fecha en que hace efectiva la cesión.

Artículo 41.- Requisitos del tratamiento de datos de carácter personal por cuenta de terceros.

El apdo. 7 actualiza la redacción del anterior artículo 36.7 DS, haciéndola más acorde con el artículo 88.5 RLOPD.

Artículo 44.- Procedimiento y efectos del ejercicio del derecho de acceso a datos de carácter personal.

En base a lo dispuesto en los artículos 17 LOPD y 25.5 RLOPD, que regulan la obligación del titular del fichero de conservar la prueba del cumplimiento del deber de respuesta, se ha incluido como trámite del procedimiento, al igual que en la cesión de datos, la firma de una comparecencia o diligencia en el momento de acceso, acreditativa de la norma o resolución administrativa en que se fundamenta, la identidad del cesionario, el dato o datos cedidos y la fecha en que hace efectiva la cesión.

Artículo 45.- Procedimiento y efectos del ejercicio de los derechos de rectificación y cancelación.

La modificación que introduce el apdo. c) de este artículo,1 incorpora la resolución de la AEPD R/01176/2010, dictada en el procedimiento nº AP/00098/2009.

Artículos 47-50.- Certificados de Firma Electrónica.

De nueva incorporación, contienen una regulación mínima, hasta ahora inexistente, tanto del régimen de constitución y de adscripción de las Oficinas municipales de Registro como de los registradores de Firma Electrónica. Así como de los procedimientos de expedición de Certificados de Firma a los ciudadanos y a los empleados públicos sobre los que se determina la sujeción al procedimiento establecido por la FNMT-RCM para la obtención de los certificados de los ciudadanos, y acomodando la de los empleados municipales a la normativa de desarrollo de la Ordenanza Municipal de la Administración Electrónica.

ANEXOS.-

Se mantienen los incorporados al DS de 2009, con dos novedades:

1. Por su mayor utilidad, se cambia el orden de los anteriormente incorporados como anexos VI, y VII, sobre relación de los contratos de servicios vigentes y acerca de los ficheros automatizados de datos de carácter personal inscritos en la AEPD, respectivamente, que pasan a denominarse anexos I y II, respectivamente, seguidos en su orden por los restantes existentes.

2. La relación de contratos de prestación de servicios actualmente vigentes del Anexo I y el Anexo II (con los ficheros inscritos en la Agencia de Protección de Datos) no se incorporan al texto normativo del DS, sino a documentos adjuntos al mismo, por ser obligatorio mantener ambas relaciones actualizadas.

Quedando por tanto enumerados finalmente los anexos del DS con el orden siguiente:

ANEXO I. CONTRATOS DE SERVICIOS CON TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. Que incluye los formularios con las medidas de Seguridad que deben incorporar las distintas clases de contratos de servicios, más con desarrollo aparte de la tabla de los contratos vigentes, por ser preceptiva su continua actualización.

ANEXO II. FICHEROS DE DATOS DE CARÁCTER PERSONAL INSCRITOS EN REGISTRO GENERAL AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS / NIVELES DE SEGURIDAD, CÓDIGOS DE INSCRIPCIÓN Y USOS. Con desarrollo aparte, por ser preceptiva su continua actualización.

ANEXO III. DEFINICIONES, TÉRMINOS Y CONCEPTOS

ANEXO IV. REGLAS DE ASIGNACIÓN DE PERFILES

ANEXO V. ESCALA DE ASIGNACIÓN DE PERFILES

ANEXO VI. ESCALA DE NIVELES DE RESERVA

ANEXO VII. PROCEDIMIENTOS DE GESTIÓN DE COPIAS DE RESPALDO (BACK-UPS)

- DOCUMENTO MUNICIPAL DE SEGURIDAD (DOCUMENTO MODIFICADO) -

CAPITULO PRIMERO. DISPOSICIONES GENERALES

Artículo 1.- Objeto.

El presente Documento Municipal de Seguridad (en lo sucesivo, DS), tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los ficheros que contengan datos de carácter personal, así como la de los recursos del Sistema de Información Municipal (en adelante SIM) que intervengan en el tratamiento de aquellos mediante medios y técnicas informáticos, electrónicos o telemáticos.

Artículo 2.- Contenido.

1. Este DS aplica la legislación estatal sobre protección de datos adaptándola al ámbito de gestión de las competencias del Ayuntamiento de Granada. En particular, se sustenta en la LO 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), en la Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP) y reglamentos que la desarrollan.

2. Los términos y conceptos empleados en el presente DS, amoldados a las especificidades del SIM, se recogen en anexo III al mismo.

Artículo 3.- Ámbito de aplicación.

1. El DS tiene la consideración de documento de obligado cumplimiento para los servicios municipales, así como para los organismos autónomos y entidades que, mediante acceso a los recursos del SIM, traten datos de carácter personal de ficheros de titularidad municipal, y que, en adelante, serán denominados conjuntamente como Administración Municipal:

a. Los órganos administrativos que integran el Ayuntamiento de Granada.

b. Los servicios remanentes de los disueltos organismos autónomos municipales.

c. Las sociedades mercantiles de capital íntegramente municipal cuando ejerciten encomiendas de gestión.

d. Las sociedades y las entidades concesionarias o prestadoras de servicios municipales, autorizadas por el título concesional o el contrato de servicios.

2. Cuando se produzca la adaptación de los entes de gestión de servicios públicos locales al régimen previsto en la disposición final novena de la Ley 5/2010, de 11 de Junio, de Autonomía Local de Andalucía, el DS será igualmente de aplicación a los mismos.

CAPÍTULO SEGUNDO. GESTIÓN DEL S.I.M.

Artículo 4.- Desarrollo del Sistema.

1. La Delegación Municipal competente, en base a las resoluciones sobre organización y estructura de la Administración municipal ejecutiva, ostenta la dirección de la organización, gestión y control de los proyectos y trabajos relativos a las tecnologías de la información y de las comunicaciones que se realicen en el ámbito de la Administración Municipal, en consonancia con la legislación vigente de aplicación.

2. Al personal adscrito a los servicios informáticos (Centro de Proceso de Datos; en lo sucesivo, CPD) le corresponden las funciones que le son propias a los puestos de trabajo de desempeño, según lo dispuesto en los artículos 15 y concordantes DS.

3. Por la Delegación competente se autorizará el acceso al sistema de desarrollo del software. Dicha autorización se entiende implícita para el personal adscrito al CPD que realice funciones de análisis, diseño e implementación de objetos de aquel.

Artículo 5.- Usuarios del SIM.

Son usuarios del SIM los de la Administración Municipal expresamente autorizados, conforme al presente DS, para acceder a las aplicaciones, programas y ficheros y para utilizar elementos de software o hardware específicos, en consonancia con las exigencias que requiera el desempeño de sus funciones.

Artículo 6.- Identificación y autenticación de usuarios.

1. La conexión a los distintos componentes del SIM precisa la identificación y la autenticación del usuario. En los procedimientos electrónicos la identificación y la autenticación se efectuarán por los sistemas de identificación electrónica establecidos conforme a la Ordenanza Municipal de Administración Electrónica. En los restantes accesos al SIM, la identificación y autenticación se efectuarán mediante el número de usuario (el de Personal) más una contraseña. La contraseña inicial de los usuarios de nuevo ingreso será su primer apellido, que deberán modificar según apdos. 7 y 8 del presente artículo.

2. El identificador faculta el acceso al disco duro de la CPU del equipo asignado, a la carpeta del Servidor de Ficheros abierta con el mismo número en el servicio de adscripción (carpeta del usuario), a la carpeta Unidad, a las compartidas y a las restringidas del Área o Servicio en dicho servidor para las que tenga autorización. También identificarán y autenticarán al usuario en las aplicaciones del Servicio

de Información Municipal (S.I.M.), en el programa de comunicaciones internas (Intranet) y ante el Centro de Atención a Usuarios (CAU).

3. El personal procedente de los disueltos organismos autónomos municipales, y el de las empresas, agencias y entidades públicas empresariales municipales, que hubiera accedido con anterioridad al SIM, conservará el mismo identificador de anteriores accesos, con los rangos numéricos ya asignados. A los que no hubieran accedido se les asignará el correspondiente identificador, según el apdo. 1 del presente artículo.

4. El personal de las entidades contratadas para tratamiento de datos por cuenta del Ayuntamiento dispondrá de un código especial y único de usuario del sistema.

5. Siempre que su régimen de adscripción al Ayuntamiento lo permita, el personal becario de investigación, en prácticas, de colaboración social y asimilado, tendrá competencia de ejecución y de consulta sólo a ficheros de nivel Básico; salvo a los datos del Padrón Municipal de Habitantes, a los que podrán acceder únicamente en régimen de consulta, y a los gestionados en el CPD, que tratarán exclusivamente en el entorno de Desarrollo.

6. Es preceptivo usar, mantener actualizadas y guardar la confidencialidad de las claves o contraseñas personales que garantizan la autenticación del usuario.

7. El modelo de contraseña adoptado es el de contraseña simple para acceso a los distintos componentes del SIM.

8. La contraseña inicial debe ser cambiada por el usuario en la sesión inaugural. La única operación permitida una vez producido el primer acceso al sistema será la modificación de dicha contraseña. Se arbitrarán las medidas que impidan cualquier otra operación en tanto la contraseña inicial permanezca inalterada. Para el cambio de contraseña el usuario deberá introducir una secuencia de caracteres que únicamente su propietario podrá conocer.

9. Las contraseñas se almacenarán en el sistema de forma ininteligible.

10. Las contraseñas tendrán una validez máxima de un año desde su establecimiento.

Artículo 7.- Gestión de las autorizaciones de acceso.

1. Por la Delegación que ostente las competencias en materia de Personal se facultará la autorización descrita en el artículo 6, así como el identificador y la contraseña en los mismos señalados.

2. Automáticamente se asignará al usuario en el Servidor de Ficheros una carpeta de usuario dentro del servicio de adscripción, con número de identificador único, a los solos efectos de registro y custodia de las actuaciones informatizadas que deba realizar por razones de servicio. En dicha carpeta

no podrán grabarse datos estrictamente personales, que lo serán en su caso en el disco duro local con sujeción a las limitaciones y requisitos del artículo 8 DS.

3. Simultáneamente, se dará de alta al usuario-a en la carpeta G-Unidad del servicio de adscripción, para los usos y finalidades regulados en el artículo 8.15 DS.

4. Se arbitrarán procedimientos de revocación-suspensión de autorizaciones de accesos a los usuarios en interrelación con la aplicación de Nóminas, que automaticen los accesos a las aplicaciones y carpetas, así como los perfiles asignados.

5. Sin perjuicio de lo dispuesto en apdos. 1 a 3, hasta tanto se implementa el procedimiento descrito en el apartado anterior, la asignación, modificación y revocación de autorizaciones se adecuará al siguiente procedimiento:

a. Las peticiones de acceso de los usuarios a carpetas de bases de datos y aplicaciones, se cursarán por la correspondiente Jefatura de Unidad al Centro de Atención a Usuarios (C.A.U.), preferentemente a través del teléfono 6505, o bien a la dirección electrónica cau@granada.org o a la dirección web http://cau:8181. El mismo procedimiento se seguirá para las peticiones de software y de recuperación de ficheros, regulada en el artículo 8.4 DS

b. Las necesidades de hardware se cursarán por las Jefaturas de Unidad a la dirección electrónica institucional del personal de la Subdirección de Infraestructura CPD.

c. Las averías y las incidencias generales por avería de los equipos, se comunicarán directamente por los usuarios al Centro de Atención a Usuarios (C.A.U.), preferentemente a través del teléfono 6505, o bien a la dirección electrónica cau@granada.org o a la dirección web http://cau:8181.

d. La renovación por caducidad de las autorizaciones de acceso a las aplicaciones se solicitará, asimismo directamente por los usuarios, a la dirección electrónica institucional del personal del Gabinete de Seguridad.

e. Las incidencias de datos de carácter personal, reguladas en los artículos 8.5 y 42 DS, así como los daños, las desapariciones y los usos indebidos o no autorizados de los equipos y programas, se comunicarán por los mismos usuarios, mediante informe detallado, al Responsable de Seguridad CPD.

f. El material fungible (*pen drive*, CD, DVD, tóner o cartuchos de impresoras) se solicitará por los usuarios a la dirección electrónica institucional del personal del Servicio de Organización.

6. Las peticiones serán motivadas y señalarán, en su caso, el núm. de usuario-a, las funciones que desempeñe, los trámites, utilidades, carpetas o recursos a los que deba acceder (o la identificación del grupo de asimilación) y, de ser previsible, la fecha de la finalización o suspensión de funciones.

7. Tratándose de personal de nuevo ingreso, así como del trasladado de Área o Servicio por cambio de puesto, se interesará por el mismo procedimiento de los apdos. anteriores la configuración personal del usuario en el equipo asignado, así como, en su caso, el alta en las carpetas de red y cuenta de correo electrónico.

Artículo 8.- Obligaciones de los usuarios del SIM.

Son obligaciones generales de los usuarios del SIM, cualquiera sea su vinculación con el Ayuntamiento de Granada o el puesto de desempeño, las siguientes:

1. Obtener autorización formal antes de acceder a o de utilizar cualquier activo de información o recurso de software o hardware del SIM conforme al procedimiento regulado en el artículo 7 DS.

2. Aplicar los recursos informáticos al ejercicio de las funciones y obligaciones que les correspondan en el ámbito de la relación de servicio o de confianza contractual asumida. Los accesos de los usuarios serán registrados y controlados según se establece en el capítulo V y quedan sujetos a responsabilidad, distinguiéndose entre la competencia de consulta y la de ejecución.

3. Comunicar personalmente las averías de los equipos al Centro de Atención a Usuarios (C.A.U.) a través del teléfono 6505, o bien por e-mail a la dirección electrónica . A cada incidencia se le asignará un número de referencia de control que será comunicado al peticionario, al Gabinete de Seguridad CPD y a los técnicos municipales en su caso.

4. Comunicar de forma inmediata la necesidad de recuperar los datos de carácter personal o de cualquier otra naturaleza, eliminados por error de manipulación o por avería técnica de grabación, por mediación de la Jefatura de Unidad, al Centro de Atención a Usuarios (C.A.U.), a través del teléfono 6505, o bien por e-mail a la dirección electrónica cau@granada.org o a la dirección web http://cau:8181. La recuperación se atendrá al procedimiento que corresponda de los artículos 20.3 ó 20.4 DS.

5. Comunicar personalmente al Gabinete de Seguridad CPD, mediante informe detallado, la pérdida, extravío, desaparición o uso indebido o no autorizado de elementos de hardware, o de software, o de datos de carácter personal obrantes en ficheros de titularidad municipal, para su tramitación como incidencia de datos de carácter personal conforme al procedimiento del artículo 42 DS. Se considerará incidencia de datos de carácter personal todo acontecimiento que haya puesto, ponga o pueda poder en riesgo la seguridad y/o la integridad de estos datos, cualquiera sea el soporte o medio de difusión o de tratamiento de los mismos.

6. Informar a su Jefatura de Unidad cuando termine la necesidad de acceder a cualquier activo de información o de usar los elementos de software o los recursos de hardware asignados.

7. Usar y mantener actualizadas las claves o contraseñas personales que garantizan la autenticación del usuario, así como guardar la confidencialidad de las mismas.

8. Cerrar o, en su caso, bloquear el equipo, cuando no esté en uso o haya finalizado el motivo del acceso, al objeto de evitar accesos no deseados. A tal fin, la activación del protector de pantalla, la confirmación de usuario o la configuración de energía del sistema operativo instalado, correrán por cuenta del usuario y serán de su exclusiva responsabilidad. Las cuestiones que se susciten para su implantación serán formuladas directamente por los usuarios mediante llamada telefónica al Centro de Atención a Usuarios (C.A.U.). Si la deficiente implantación de las mismas afectara a la seguridad y/o integridad de los datos de carácter personal, se tramitarán las correspondientes incidencias de datos de carácter personal conforme a los artículos 8.5 y 42 DS.

9. Custodiar los recursos informáticos y evitar el deterioro, extravío, hurto o robo tanto de los equipos (unidades CPU, periféricos e impresoras) como de los soportes utilizados, adoptando las medidas de Seguridad Física a su alcance en cuanto a su ubicación, protección y custodia (puertas, cerraduras, fuentes de calor, humedad, etc.), cuya implantación correrá por cuenta del usuario y serán de su exclusiva responsabilidad. A tal fin, las dependencias deberán estar siempre cerradas bajo llave fuera de las horas de servicio, correspondiendo el control de las llaves o sistemas de acceso a las Jefaturas correspondientes. Las cuestiones que se susciten en la implantación de dichas medidas serán formuladas directamente por los usuarios al Servicio de Organización o a la Policía Local. Si la deficiente implantación de las mismas afectara a la seguridad y/o integridad de los datos de carácter personal, se tramitarán las correspondientes incidencias de datos de carácter personal conforme a los artículos 8.5 y 42 DS.

10. Conocer la clasificación, en cuanto a los niveles de seguridad asignados, de los activos de información que gestiona.

11. Conocer y aplicar las medidas de seguridad implantadas que afecten al desarrollo de sus funciones, así como las consecuencias que pudieran derivarse de su incumplimiento.

12. Conectarse durante la sesión de trabajo, a través de la cuenta de correo descrita en el artículo 13 DS, al programa de comunicaciones internas (Intranet), al objeto de recibir y emitir comunicaciones sobre cuantas resoluciones, instrucciones, documentos, avisos y mensajes de correo electrónico sean necesarios para el funcionamiento del sistema y la prestación de los servicios, con las limitaciones y requisitos de los artículos 13 y 14 DS y las instrucciones y circulares que al efecto se dicten.

13. No transgredir ningún procedimiento de control establecido, quedando terminante prohibido:

a. La suplantación de contraseñas personales.

b. La transgresión de las autorizaciones de acceso a aplicaciones, programas, equipos y soportes en relación con las funciones del usuario en el servicio de su adscripción.

c. La utilización de cualesquiera de estos recursos para finalidades distintas para las que fueron desarrollados y concedidos.

d. La instalación y uso de cualesquiera recursos informáticos no expresamente autorizados.

14. Guardar secreto de los datos de carácter personal de los que se tenga conocimiento por razón del servicio, sin perjuicio de las transcripciones que resulten necesarias en los procedimientos de gestión de expedientes, a los informes y resoluciones administrativas, legalmente procedentes.

15. Evitar el tratamiento en las carpetas personales de G:\Unidad de toda la información de datos de carácter personal, o de naturaleza técnica o institucional, que sea inadecuada, excesiva, innecesaria o desfasada, limitando su uso a la finalidad de intercambiar o depositar temporalmente información cuando ésta no pueda transmitirse por otros medios de la Intranet municipal, como el intercambio de ficheros o los ficheros anexos a mensajes de correo electrónico. La información deberá permanecer en G:\Unidad el menor tiempo posible, por lo que se procederá a extraerla e incorporarla o a un dispositivo o a una ubicación seguros de acceso restringido, o a suprimirla con periodicidad mensual, bien por el propio usuario, bien por los servicios del CPD por razones técnicas. A tal fin, la puesta a disposición de información y documentación en las carpetas personales del personal referido en el artículo 6.5 DS, concerniente a los ficheros que en el citado precepto se describen, y su posterior supervisión y recuperación, serán responsabilidad de las Jefaturas de Unidad correspondientes.

16. Las Jefaturas de Unidad instruirán al personal a su cargo sobre las anteriores obligaciones y las reguladas en la normativa de protección de datos, e informarán puntualmente al Gabinete de Seguridad de las anomalías que detecten, proponiendo, en su caso, las medidas a adoptar. El incumplimiento de las citadas obligaciones se dirimirá con arreglo al régimen disciplinario de las Administraciones Públicas, y dará lugar a la exigencia, en su caso, de las responsabilidades administrativas que correspondan, sin perjuicio de las de índole civil o penal, de las que se deriven de las incidencias de seguridad o de las actuaciones de la Agencia Española de Protección de Datos.

Artículo 9.- Caducidad, suspensión y revocación de autorizaciones.

1. Las autorizaciones de acceso a los recursos informáticos del personal temporal caducarán en la fecha de finalización de la relación laboral o de servicio.

2. Quedará suspendida la autorización de acceso al SIM del personal con interrupción de relación laboral o de servicio activo mientras se mantenga ésta, procediéndose a su levantamiento cuando finalice la misma.

3. Se revisarán las autorizaciones cuando el usuario sufra un cambio de plaza o puesto en la organización.

4. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información a un máximo de cinco intentos. Una vez agotados los mismos, la conexión quedará bloqueada y la autorización será revocada.

5. El personal de entidades contratadas en régimen de prestación de servicios conforme al artículo 41, sólo accederá a los recursos estrictamente referidos en el respectivo contrato y por el tiempo y conforme a los requisitos en el mismo estipulados.

Artículo 10.- Tablón Electrónico.

1. La publicación en el Tablones de Edictos Electrónico de los actos, los acuerdos y las resoluciones de carácter general de la Administración Municipal, es preceptiva, además de para los que deban serlo por mandato legal o reglamentario, para todos los que se remitan para su publicación a los boletines oficiales (artículo 59.5 LRJPAC).

2. La publicación en el Tablón Electrónico ha de efectuarse en plazo de cinco días desde su adopción. Los documentos se remitirán como anexos de correo electrónico en el citado plazo, o, en todo caso, en el momento de su envío al boletín o boletines oficiales correspondientes, a edictos@granada.org. En la remisión, se señalará el plazo de exposición, con indicación de la fecha de inicio y final de la misma. Cuando se trate de expedientes sancionadores el plazo de exposición será el de veinte días establecido en el artículo 29.10 DS.

3. Las resoluciones administrativas que habrán de publicarse en el Tablón Electrónico, son, entre otras, con el formato que se señala para cada supuesto, las siguientes:

3.1 De forma disociada, según los artículos 61 LRJPAC y 29.3 DS: las de toda clase de expedientes sancionadores, las de expedientes con datos de carácter personal sensibles o especialmente protegidos o que formen parte de ficheros de nivel Alto, según lo dispuesto en el artículo 32.5 DS, las resoluciones que lesionen derechos o intereses legítimos, las resoluciones administrativas particulares (subvenciones, licencias, autorizaciones, etc.) que hayan de publicarse en sustitución de la notificación o cuando se acuerde la misma de conformidad con el artículo 60 de la LRJPAC, los listados de resultados de procesos selectivos y los órdenes del día y las Actas del Ayuntamiento Pleno, conforme a lo regulado en el artículo 70.1 de la LRBRL.

3.2 Mediante copia digital íntegra del documento: las disposiciones administrativas generales (Ordenanzas, Reglamentos, Decretos, Edictos, Bandos) y aquellos actos cuya publicación sea obligatoria por disposición legal expresa (entre otros, los regulados en el artículo 54 Ley 5/2010, de 11 de Junio, de Autonomía Local de Andalucía).

3.3 Los anuncios de otras Administraciones en formato papel o electrónico recibidos en el Registro General o en el Registro Electrónico General, se remitirán inmediatamente al personal referido en el apdo. 2 para su digitalización y publicación en el Tablón Electrónico. A los de carácter sancionador les será de aplicación el artículo 29.10 DS sobre el plazo de exposición y el apartado 3.1 del presente artículo en cuanto al contenido.

Artículo 11.- Tablón del Empleado.

1. El Tablón del Empleado es una base de datos de la Intranet municipal con información de interés para los empleados del Ayuntamiento de Granada, de acceso exclusivo por y para los mismos. Por lo que los anuncios publicados identificarán inequívocamente a su autor en la ventana visible del propio anuncio.

2. El Tablón no podrá incluir anuncios con mensajes o noticias de contenido político (prohibidos por acuerdo plenario núm. 752 de 30/09/2011), con publicidad no solicitada (*spam*), que avisen de la instalación de virus, gusanos o troyanos, ni los que informen de campañas de solidaridad que no identifiquen al autor y fines de la página Web o no vayan avalados por una organización prestigiosa o no indiquen la fecha de la finalización de aquella (*hoax*).

3. El Tablón se estructura en las cuatro secciones informativas siguientes, con los contenidos que se describen para cada una de ellas. Dichos contenidos son excluyentes, de forma que la inserción de un anuncio en una sección impedirá su publicación en las restantes. La duplicidad del anuncio en más de una sección se deducirá de su contenido y, de coincidir éste, el Gabinete de Seguridad CPD mantendrá aquel en la sección que corresponda y lo suprimirá en las restantes.

3.1 Información General del Tablón del Empleado.

Esta sección publicará la información de interés general que difundan los propios usuarios del SIM sobre todo tipo de contenidos, siempre que los anuncios insertados cumplan taxativamente los requisitos y las limitaciones del presente artículo e identifiquen al propio usuario como único interlocutor de contacto. A cuyo fin, las referencias del anuncio a un número de teléfono o dirección electrónica de contacto, serán exclusivamente los asignados a los empleados municipales en la Intranet Municipal, no pudiendo incluir datos de terceros para contactar o intercambiar información, salvo en los anuncios sobre actividades culturales que deban incluir números de teléfono, direcciones electrónicas o páginas web a la sola finalidad de ampliar la información o de facilitar la inscripción de los posibles participantes en las mismas.

3.2 Sección de Información de Servicio del Tablón del Empleado.

Contendrá la información elaborada o difundida por el personal del órgano encargado de coordinar la información municipal, adscrita a la Delegación competente, conforme al artículo 4 DS, con instrucciones que afecten o repercutan en el normal desempeño del puesto de trabajo, sobre, entre otras, las siguientes materias: organización, incidencias de la red telefónica, noticias sobre prevención de riesgos laborales y vigilancia de la salud, cambios en dependencias municipales, incidencias en la red de comunicaciones, utilización de los recursos de hardware y software, comunicaciones de Seguridad que deban publicarse, y las que afecten al mantenimiento de edificios, cortes de suministro eléctrico, realización de obras y reparaciones, fumigaciones, modificación de horarios en el servicio de lanzadera, etc. Las comunicaciones emitidas por esta sección tendrán carácter oficial.

3.3 Sección Institucional del Tablón del Empleado.

Para la difusión por la Delegación competente, conforme al artículo 4 DS, y/o las personas por la misma autorizadas, de anuncios institucionales con información relevante para el servicio en forma de órdenes, instrucciones y circulares. Las comunicaciones emitidas tendrán carácter oficial, sin perjuicio de su transmisión por canales convencionales y por mensajes de correo masivos de la Intranet y *Web-mail*.

3.4 Información Sindical del Tablón del Empleado.

Insertará la información de interés general para el personal municipal que precisen difundir la Junta de Personal y el Comité de Laborales del Ayuntamiento de Granada, así como las secciones sindicales con representación en estos órganos. Siendo los contenidos que se inserten de la exclusiva responsabilidad de las entidades anunciantes.

4. Los anuncios y los enlaces a los mismos incorporados que incumplan las limitaciones señaladas en los apdos. anteriores, en lo que les resulte aplicable, así como los de carácter ofensivo hacia personas o colectivos y los difundidos mediante el empleo de pseudónimos, serán borrados de oficio por el Gabinete de Seguridad, comunicándose su eliminación al autor de los mismos. Las reclamaciones que en su caso se formulen a raíz de la supresión, se resolverán por la Delegación competente para el desarrollo del Sistema, según el artículo 4 DS.

5. La cesión, comunicación o tratamiento de la información del Tablón por cualquier medio (inclusive teléfono, fax, correo electrónico y medios de comunicación), queda sujeta a las limitaciones, principios y garantías de la legislación vigente sobre protección de datos de carácter personal y precisa autorización expresa de los afectados, con exigencia, respecto a los presuntos infractores, de las responsabilidades disciplinarias y de otra índole a que haya lugar.

Artículo 12.- Portal del Empleado.

El Portal del Empleado es una base de datos de los anuncios y contenidos del artículo 11.3.2 DS que se pongan a disposición de los empleados municipales en la Intranet municipal, y el sitio de la Sede Electrónica de la Administración Municipal, para acceso del personal municipal, mediante Firma Electrónica, tanto a los citados contenidos como a los siguientes: correo electrónico, consulta de nóminas, teleformación, Tablón del Empleado, permisos y licencias, teléfonos internos, actas íntegras de las sesiones del Excmo. Ayuntamiento Pleno y Callejero de Granada.

Artículo 13.- Uso del correo electrónico.

1. En el uso del correo electrónico se preservará el derecho al secreto de las comunicaciones respecto al contenido de los mensajes; no así en cuanto al control de remitente y destinatarios, cuyas cuentas de correo quedarán claramente consignadas y registradas a los efectos procedentes.

2. Por razones de seguridad, se prohíben las cuentas de correo distintas a la habilitada en la Intranet mediante el software normalizado o programa de comunicaciones internas instalado en el equipo facilitado al usuario, con la salvedad de los usuarios expresamente autorizados por necesidades del servicio para el uso de otras cuentas.

3. El programa de comunicaciones internas y las cuentas de correo en el mismo habilitadas, descritos en el apartado anterior, constituyen el entorno cerrado de comunicación de la Administración Municipal (Intranet Municipal). Los documentos electrónicos transmitidos por el mismo serán válidos a todos los efectos.

5. Para evitar la sobrecarga de la Intranet que ocasionaría el reenvío entre los usuarios de mensajes innecesarios o con información no contrastada y, por ende, de escasa o nula veracidad, bajo ningún pretexto se deben abrir, contestar ni reenviar los mensajes siguientes:

a. Los mensajes de remitente desconocido y, especialmente, los anexos a los mismos, cuya recepción no haya sido previamente concertada por otros medios (v., por teléfono, carta, comunicación, oficio, etc.).

b. Los que contengan publicidad comercial no solicitada (*spam*).

c. Los no procedentes del CPD que avisen de la instalación de virus, gusanos o troyanos.

d. Los que informen de campañas de solidaridad que no identifiquen al autor y fines de la página Web, no vayan avalados por una organización prestigiosa o no indiquen la fecha de la finalización de aquella (*hoax*).

e. Todos los mensajes y anexos de correo de contenidos *spam* y *hoax* deben ser borrados de inmediato de la bandeja de entrada de la cuenta del usuario, sin abrirlos.

Artículo 14.- Acceso a datos de carácter personal en la atención personalizada de las oficinas municipales y transmisores por Internet, correo electrónico, soportes, vía telefónica o fax.

1. Únicamente el interesado o su representante legal pueden obtener datos de carácter personal referidos al titular que obren en cualquier documento o fichero municipal (inclusive los concernientes a acreedores o a deudores de la Hacienda Municipal). Para ello, tanto si procede facilitaros por la atención personalizada en oficinas municipales, como si han de ser remitidos por cualquier otro medio (incluso fax), deberá cumplimentarse siempre el procedimiento de ejercicio del derecho de acceso regulado en el capítulo XI DS. En las comunicaciones telefónicas, el personal Encargado del tratamiento contrastará previamente las claves o contraseñas en su caso concertados con el interesado; o identificará con el máximo rigor al titular de los datos mediante los ficheros municipales de consulta.

2. Para la difusión de documentos que contengan datos de carácter personal por canales de información no implantados en la Sede Electrónica Municipal (como Internet, correo electrónico

externo, anexos de correo electrónico externo o soportes), será imprescindible la autorización de la Dirección General o Jefatura de Servicio para cada comunicación, salvo que los datos hayan sido disociados según el procedimiento del artículo 29.3 DS, o se trate de publicaciones preceptivas en medios de comunicación social y boletines oficiales. En las cesiones de datos, se estará a lo dispuesto en el capítulo VIII DS. En los restantes supuestos deberán cumplirse los procedimientos del capítulo XI DS sobre ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los titulares o afectados.

CAPÍTULO TERCERO. ÓRGANOS DE GESTIÓN DEL S.I.M.

Artículo 15.- Centro de Proceso de Datos.

1. Dependencia municipal donde se traten automatizadamente datos. Los centros de tratamiento del Centro de Proceso de Datos (CPD) se distribuyen en tres grupos de áreas:

1.1 Áreas abiertas: dependencias municipales donde se ubican los equipos informáticos destinados a la prestación de servicios municipales.

1.2 Áreas limitadas: dependencias municipales antesalas de las áreas controladas y/o que almacenan soportes informáticos.

1.3 Áreas controladas: dependencias donde se ubican los equipos centrales del SIM. Se subdividen en:

1.3.a Área restringida: recinto donde se encuentran los equipos centrales, servidores y sistemas de comunicaciones.

1.3.b Áreas internas: resto de zonas del CPD donde habitualmente presta servicio el personal adscrito al mismo, sin incluir el área limitada.

2. La gestión de los recursos del SIM requiere la estrecha colaboración entre el personal del CPD y las distintas Áreas o Servicios, que colaborarán en las tareas de actualización permanente de la información y de los servicios que se acuerde difundir o prestar a través de la Intranet o de redes abiertas o cerradas de comunicación (Internet). A tal efecto se seguirán las directrices de la Comisión de Coordinación de los Sistemas de Información o del órgano municipal que le sustituya, especialmente las que se dicten en materia de seguridad.

3. El personal del CPD es primordialmente responsable de la confidencialidad o deber de guardar secreto de los datos de carácter personal de los ficheros municipales automatizados, por lo que queda sujeto a las siguientes obligaciones:

3.1 Gestionar los certificados de los servidores y proveer permanentemente la funcionalidad y el buen estado de servidores, redes, equipos centrales y de comunicación.

3.2 Impedir la difusión de cualquier información que pueda poner en peligro la integridad u óptimo rendimiento tanto de los sistemas y equipos como de la información tratada. Por ello, toda documentación elaborada para dar a conocer procedimientos sobre acceso y bloqueo de los mismos tendrá la consideración de información reservada, arbitrándose soluciones técnicas adecuadas para garantizar su seguridad.

3.3 Adoptar las medidas necesarias para que todos los usuarios del SIM conozcan las normas que deben aplicar en el desarrollo de sus funciones, así como las consecuencias que pudieran derivarse en otro caso y las responsabilidades en que podrían incurrir.

3.4 Mantener actualizada la relación de usuarios que tengan acceso autorizado al sistema de información a partir de la información facilitada por el Área Personal o la que tenga atribuida la gestión de los recursos humanos municipales.

3.5 Establecer procedimientos de identificación y autenticación para dicho acceso.

3.6 Establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

3.7 Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos regulados en este DS, así como de los de identificación de soportes, su almacenamiento, registro y gestión.

Artículo 16.- Administradores.

1. Son Administradores del SIM, cualquiera sea su adscripción orgánica o funcional, los súper usuarios con funciones de alta, baja y asignación de niveles de perfil en una o varias aplicaciones, carpetas o ficheros, respecto a otros usuarios, bajo la supervisión del Gabinete de Seguridad

2. Son Administradores especiales:

a. Las Direcciones Generales para disponer las altas y bajas de los usuarios en la carpeta o carpetas restringidas y compartidas y en las aplicaciones de sus respectivos servicios.

b. Las distintas Jefaturas de Unidad para disponer las altas y bajas de los usuarios en la carpeta o carpetas compartidas y en las aplicaciones de sus respectivos servicios.

c. Los-as Directores-as de los CCMMSS respecto al fichero “Sistema de Información de Usuarios de Servicios Sociales (SIUSS)” y a la aplicación “Derivación de Casos de Violencia de Género”.

d. La Jefatura del Centro de Atención a la Mujer sobre el fichero “Violencia de Género”.

e. La Jefatura del Centro de Medicina de Empresa para el fichero de “Vigilancia de la Salud de los Empleados Municipales”.

f. La Dirección General del Área de Economía y Hacienda sobre el fichero de Contabilidad.

g. La Dirección General de Personal respecto de los ficheros “Control de Personal” y “Nóminas”.

h. La Subdirección de Recursos Lógicos Corporativos sobre el fichero “Gestión de Datos Básicos”.

3. Son Administradores Generales del SIM, con funciones de auditores-colaboradores del Gabinete de Seguridad, conforme al Organigrama Funcional y RPT vigentes, los Administradores del CPD, con las funciones y la adscripción orgánica que se señalan:

3.1 Adscritos a la Subdirección de Infraestructura CPD:

3.1.1. Administrador de Bases de Datos. Funciones: comunicar con los usuarios de la base de datos y responsables del sistema; detectar necesidades de uso, roles, privilegios, etc.; determinar la interfaz de conexión con otros sistemas existentes; identificar recursos hardware y software disponibles en la organización y en su caso adoptarlos o proponer su ampliación y/o mejora; determinar la infraestructura de red existente y su posible ampliación en función de las nuevas demandas; planificar, diseñar e implementar los sistemas de bases de datos; establecer normas y procedimientos para controlar la seguridad y la integridad de los datos de forma eficiente; mantener la disponibilidad de los datos; ejecutar los procedimientos de recuperación ante posibles pérdidas de información; desarrollar y ejecutar los *scripts* para migración a sistemas de almacenamiento de la información; mantener y optimizar las bases de datos; crear nuevos usuarios, grupos, roles, etc.; gestionar el almacenamiento de la base de datos; y recuperar el Sistema de Bases de Datos tanto de los fallos del sistema como de los medios de almacenamiento.

3.1.2 Administrador de Sistemas. Funciones: realizar copias de respaldo y de seguridad de sistemas, ficheros, bases de datos y de acceso a Internet; almacenar y gestionar los *back-ups*; instalar y administrar los sistemas operativos (usuarios, red, servicios); gestionar los servidores de ficheros; diseñar, planificar y documentar los procedimientos de obtención-recuperación de *back-ups*; instalar Windows e implementar Active Directory; instalar y configurar Linux; configurar el Servidor de Ficheros; asignar privilegios a las carpetas del Servidor de Ficheros; administrar los sistemas de virtualización y los escritorios virtuales; y administrar y gestionar *Blade-Center*.

3.1.3 Administrador de Red. Funciones: administrar, mantener y desarrollar la infraestructura de red en los niveles de enlace, red y transporte; implementar la seguridad en los tres niveles; documentar e inventariar los equipos conectados a la red, las IP y los servicios utilizados por cada máquina de la red corporativa; implantar los mecanismos de autentificación, autorización y auditoria de maquinas conectadas a la red municipal; configurar el mapa de uso de protocolos y aplicaciones; implantar los mecanismos de autentificación, autorización y auditoria de usuarios con certificación digital; y

configurar e implementar los mecanismos de detección de incidencias e intrusos y de respuesta preactiva de la Redel nivel de enlace de datos.

3.2 Adscritos a la Subdirección de Administración Electrónica CPD:

3.2.1 Administración del Servidor Web. Funciones: configurar y mantener la Web Server (Domino e IIS) en coordinación con Subdirección de Infraestructura; controlar y corregir estado de los servidores; analizar el tráfico del correo electrónico y solucionar los problemas detectados; analizar la adecuación de las medidas de protección; detectar y neutralizar los ataques; analizar los accesos al Web; gestionar los certificados electrónicos y de Administración Electrónica de los servidores; estudiar y corregir los errores en páginas Web; estudiar y corregir los problemas seguridad; programar las bases de datos Lotus Notes; programar ASP para IIS; programar las plantillas del SIM; realizar la Auditoría de seguridad del acceso telemático; administrar la Intranet; crear, certificar y mantener a los usuarios de la Intranet; resolver problemas en las bases de datos (de correo y otras), de certificados de Internet/Intranet, etc.; establecer programas de auditoría, control y reparación de problemas; crear y mantener cuentas y grupos institucionales; y diseñar y programar bases de datos y aplicaciones documentales de Intranet.

3.2.2 Administrador Web Master para mantenimiento de las páginas Web. Funciones: implementar el diseño de las páginas Web institucionales y de programas Web, colaborar con el "Servicio Municipal de Atención al Ciudadano" en la introducción de documentos en la Web, creación de elementos complejos, creación de libros electrónicos (pdf's), diseño de bases de datos para Internet, diseño de páginas y formularios Web y programación utilizando *html, javascript, jscript, LotusScript, vbscript, asp*, etc.

3.2.3 Administrador de Diseño Gráfico. Funciones: tratar y optimizar imágenes para el Web; crear logotipos para bases de datos; y diseñar menús, animaciones, vídeos y otros elementos gráficos y multimedia.

3.3 Los Administradores CPD no comprendidos en los apartados anteriores no realizarán función alguna en el entorno de los servidores del SIM, limitando sus actuaciones a las señaladas en el apdo. 1 del presente artículo.

4. Los Administradores deberán abstenerse de elaborar procedimientos no autorizados de acceso a los ficheros protegidos, comunicar cuándo pueden ser revocadas las autorizaciones concedidas y señalar qué ficheros o carpetas deben ser modificados o suprimidos, una vez satisfecha la necesidad para la que fueron creados, respetando el nivel de protección a los mismos asignado.

Artículo 17.- Encargados de los ficheros o tratamientos.

1. Es Encargado-a de cada fichero o tratamiento, sujeto a las obligaciones establecidas en el presente DS, todo-a usuario-a del SIM que trate datos de carácter personal de ficheros de titularidad municipal, cualquiera sea su relación con el Ayuntamiento de Granada.

2. El/la Encargado-a del tratamiento es responsable del tratamiento de los datos de carácter personal y de la custodia de los soportes que se generen o gestionen en el servicio de adscripción, estando sujeto a las obligaciones reguladas en los artículos 7.5.e y 8.5 DS y a los procedimientos de identificación y registro de soportes del capítulo VI DS. O al cumplimiento de las medidas de seguridad establecidas en las estipulaciones del respectivo contrato de prestación de servicios, con arreglo al capítulo IX DS.

Artículo 18.- Responsables de los ficheros o tratamientos.

1. El Ayuntamiento de Granada es el responsable de los ficheros o tratamientos declarados ante la Agencia Española de Protección de Datos. La responsabilidad municipal será exigible, en su caso, a los organismos y entidades de la Administración Municipal relacionados en el artículo 3 del presente DS, a los que se derivará, en su caso, en el ámbito de sus respectivas competencias.

2. Son obligaciones del responsable de los ficheros o tratamientos:

2.1 Aplicar la normativa vigente sobre protección de datos de carácter personal y ejecutar y difundir las medidas y procedimientos de seguridad de obligado cumplimiento para todos los usuarios del SIM.

2.2 Garantizar que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2.3 Establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

2.4 Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

Artículo 19.- Gabinete de Seguridad.

1. El Gabinete de Seguridad, inserto en la Dirección Técnica del CPD, estará constituido por los Responsables de Seguridad y el personal técnico, administrativo y auxiliar adscrito.

2. El Responsable de Seguridad es la persona a la que el Ayuntamiento ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables, sin que dicha designación suponga una delegación de la responsabilidad de aquel.

3. Son funciones del Responsable de Seguridad CPD:

3.1 Coordinar las Relaciones con la AEPD y entidades de seguridad y Admón. Electrónica.

3.2 Proponer y coordinar, con la Agencia de Protección de Datos, las medidas que, en materia de seguridad de datos de carácter personal, establezca la legislación vigente y el DS.

3.3 Informar los procedimientos electrónicos que se implanten.

3.4 Difundir las obligaciones de los usuarios.

3.5 Coordinar las medidas de seguridad del DS, proponer a la Delegación competente la concreción de las mismas y elaborar las instrucciones y circulares necesarias para su aplicación.

3.6 Gestionar el Registro de Incidencias y la tramitación de los expedientes generados mediante el mismo e informar de los procesos de recuperación de ficheros.

3.7 Gestionar el Registro de Accesos e inspeccionar los accesos de los usuarios del SIM a los recursos del mismo, informando de las anomalías detectadas, con especial prevención respecto a los ficheros de nivel de protección Alto.

3.8 Tramitar los procedimientos de inscripción, modificación y supresión de ficheros de datos de carácter personal.

3.9 Formar al Personal municipal sobre medios, procedimientos y medidas de seguridad.

3.10 Elaborar y actualizar la normativa interna sobre protección de datos de carácter personal y controlar su efectivo cumplimiento.

3.11 Autorizar el acceso a medios y recursos informáticos del SIM en lo que no corresponda a la Delegación competente para el desarrollo del Sistema conforme al artículo 4 DS, o a las Direcciones Generales o Servicios, reasignando las peticiones al personal del CPD o tramitando en su caso aquellas ante las autoridades referidas en apdos. 3.1, 3.2 y 3.5 del presente artículo.

3.12 Expedir los permisos escritos de acceso, a los centros de trabajo referidos en el artículo 15.1 DS, del personal no municipal autorizado para la prestación de servicios de desarrollo del sistema conforme a lo establecido en los artículos 4 y 41 DS.

3.13 Tramitar los expedientes de cesión y comunicación de datos de carácter personal, informando de las actuaciones que puedan afectar a su protección y proponiendo las medidas de seguridad a adoptar por los cesionarios.

3.14 Actualizar las medidas de seguridad de los contratos de servicios de tratamiento de datos de carácter personal por terceros y controlar su efectiva aplicación.

3.15 Gestionar los nombres de dominio de Internet.

3.15 Realizar Auditorias internas del SIM e implementar las externas, emitiendo los informes correspondientes.

3.16 Elaborar los Planes de Contingencias que se acuerde implantar y controlar su ejecución.

CAPÍTULO CUARTO. COPIAS DE RESPALDO (BACK-UPS) Y RECUPERACIÓN DE FICHEROS

Artículo 20.- Procedimientos.

1. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos tendrán la máxima prioridad y deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Es función exclusiva del personal técnico del CPD la aplicación de estos procedimientos.

2. La frecuencia con la que se llevarán a cabo las copias de seguridad se describe en el Anexo VII. Estos procesos son susceptibles de modificación en función de las disponibilidades técnicas y la necesidad de incrementar las medidas de seguridad establecidas.

3. El procedimiento de recuperación de ficheros, carpetas o datos eliminados por error de manipulación o avería, se incoará según el artículo 8.4 DS.

4. La recuperación de datos de carácter personal en los restantes casos requiere autorización expresa de la Delegación competente para el desarrollo del SIM, conforme al artículo 4 DS, y ha de efectuarse mediante el procedimiento de Incidencia de Seguridad, regulado en el artículo 42 DS.

CAPÍTULO CINCO. REGISTRO DE ACCESOS

Artículo 21.- Datos del Registro de Accesos de los usuarios del SIM.

1. De cada acceso al SIM se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, se recogerá la información que permita identificar el registro consultado o modificado.

3. El período mínimo de conservación de los datos registrados será de dos años.

Artículo 22.- Control de accesos de usuarios.

1. El control de accesos deberá estar permanentemente activado y se efectuará por el Gabinete de Seguridad.

2. El Responsable de Seguridad se encargará de revisar periódicamente la información registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. Dicho informe será de periodicidad al menos mensual para los ficheros de nivel de protección Alto.

CAPÍTULO SEIS. REGISTRO DE SOPORTES Y ACCESORIOS DE HARDWARE Y DE SOFTWARE

Artículo 23.- Limitaciones de uso de hardware y software no normalizados.

1. En base a lo dispuesto en los artículos 5 y 8 DS, se proscribe la instalación y uso en cualesquiera de los componentes del SIM de toda clase de elementos y accesorios de hardware y/o de software añadidos al equipo inicialmente asignado al usuario, que no hayan sido autorizados conforme al procedimiento regulado en el artículo 7 DS. El usuario no podrá manipular o modificar ningún programa o dispositivo del equipo, salvo las actualizaciones *on line* del software ya instalado en el equipo asignado.

2. Queda terminante prohibida la instalación de programas de control remoto apoyada en servidores externos a la red corporativa.

3. Los usuarios con acceso a las aplicaciones del Registro de Soportes ("Registro de Entrada de Soportes de DD.CC.PP. del Área/Servicio" y "Registro de Salida de Soportes de DD.CC.PP. del Área/Servicio…"), serán los únicos autorizados para el uso de puertos externos de almacenamiento masivo de la información (por USB y grabadoras de CD o DVD). Por lo que sólo los usuarios dados de alta en referidas aplicaciones podrán tener abiertos dichos puertos en los equipos, con independencia de la información tratada.

Artículo 24.- Registro de Soportes.

1. Se considera soporte informático el recurso informático, ajeno al disco duro del equipo asignado al usuario, especializado en la interconexión de hardware y orientado a la captura, transmisión o recuperación de datos, tales como discos magnéticos u ópticos, lápices de memoria, etc.

2. Los usuarios del SIM dejarán constancia en el Registro de Soportes de todos los movimientos de altas, bajas, salidas o entradas de dependencias municipales, de cualquier soporte informático que se genere en cada Área o Servicio, según lo dispuesto en los artículos siguientes. Esta obligación será especialmente exigible respecto a los soportes que contengan datos de carácter personal.

3. El soporte generado por reproducción parcial o total de otro existente habrá de ser inscrito como soporte singular en el Registro.

Artículo 25.- Estructura y contenido del Registro de Soportes.

1. El Registro de Soportes consta del Registro de Entrada y del Registro de Salida, implementados mediante las correspondientes aplicaciones informáticas para cada Área o Servicio.

2. En el Registro de Entrada de Soportes se anotarán las altas de soportes informáticos, tanto los generados para uso interno como los procedentes de otra Área o Servicio o del exterior de dependencias municipales.

3. En el Registro de Salida de Soportes se anotarán las salidas a otras Áreas o Servicios, o al exterior de dependencias municipales.

4. Mediante las utilidades habilitadas en los Registros de Soportes se grabarán como anexos los contenidos documentales de los soportes registrados (de ser necesario, mediante ficheros anexos y comprimidos), procediéndose a continuación a destruir o inutilizar físicamente el soporte de origen, salvo que esté prevista su remisión inmediata a terceros. De no ser posible anexar el soporte al Registro, éste será identificado y custodiado según se dispone en el artículo 26.2 DS.

5. Los soportes de ficheros de nivel Alto estarán cifrados o incorporarán algún mecanismo que garantice que la información que contienen no sea accesible ni manipulada.

Artículo 26- Identificación y custodia de soportes.

1. Los soportes de disco externo (CD ó DVD), se identificarán con el número asignado en el Registro de Soportes (número de soporte y año), que quedará impreso mediante anotación indeleble en el propio soporte junto a un resumen de los datos de carácter personal que contiene, coincidentes en todo caso con los registrados.

2. Cuando por razones técnicas no sea posible la anexión de los datos contenidos en el soporte, al Registro de soportes, según lo dispuesto en el artículo 25.4 DS, el soporte deberá quedar custodiado en emplazamiento cerrado al que sólo tengan acceso el usuario o usuarios habituales, impidiéndose su uso por personas no autorizadas.

3. La salida, fuera de dependencias de la Administración Municipal, de soportes que contengan datos de carácter personal, debe ser autorizada según lo dispuesto en el artículo 14.2 DS. Para la entrega del soporte deberá cumplimentarse la comparecencia descrita en el artículo 40.1 DS.

4. Todos los soportes quedan sujetos a los procedimientos de control de Auditoria interna y externa establecidos en el capítulo XIII DS.

5. La substracción, deterioro o pérdida de cualquier soporte de datos de carácter personal, se gestionará como Incidencia de datos de carácter personal, conforme al artículo 41 DS.

CAPÍTULO SIETE. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Artículo 27.- Datos de carácter personal.

Son datos de carácter personal los contenidos en ficheros automatizados de datos de esta naturaleza, que se describen en la tabla de definiciones del Anexo III DS, y a cuyo tratamiento le son de aplicación los principios, garantías, medidas y procedimientos de la legislación vigente sobre protección de datos de carácter personal y este DS.

Artículo 28.- Datos de acceso público.

Son datos de acceso público o datos accesibles al público, cuya consulta puede realizar cualquier persona, las publicaciones de resoluciones y acuerdos municipales en boletines oficiales y medios de comunicación; sin perjuicio, no obstante, de que a las mismas se les aplique, cuando proceda, el procedimiento de disociación de datos de carácter personal del artículo 29.3 DS.

Artículo 29.- Principios y deberes generales del tratamiento de datos de carácter personal: procedimiento de disociación de los datos; deber de confidencialidad; información y consentimiento de los afectados y publicación de datos de expedientes sancionadores.

1. Es tratamiento de datos cualquier operación o procedimiento técnico, automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación o supresión, así como las cesiones de datos que resulten de las comunicaciones, consultas, interconexiones y transferencias de datos de carácter personal.

2. Los datos de carácter personal que deban ser tratados, serán los mínimos imprescindibles que permitan la cumplimentación del trámite y exija la normativa de aplicación, preservando su confidencialidad.

3. Las unidades administrativas responsables de la tramitación de los procedimientos aplicarán en todo tratamiento de datos –especialmente en las comunicaciones no seguras por Internet, en los documentos a insertar en el Tablón Electrónico y en los anuncios a publicar en los medios de comunicación social– el procedimiento de disociación, consistente en la fragmentación y/o generalización de los datos de carácter personal o en la sustitución de los mismos (en especial los relativos a nombre, apellidos, DNI/NIF/Pasaporte/NIE, domicilio, dirección electrónica, ideología, afiliación sindical, religión, creencias, salud, origen racial, vida sexual, datos bancarios, datos familiares, profesión u oficio y estado civil), por iniciales, signos o espacios en blanco, que, sin desvirtuar el contenido de la resolución o acuerdo, impidan o dificulten la identificación del titular de los datos en ulterior tratamiento.

4. El tratamiento de datos de carácter personal de ficheros de nivel de protección Alto precisa el consentimiento expreso y por escrito de los afectados, sin perjuicio de lo contemplado en los apdos. 6 a

10 del presente artículo, o aquellos en que el tratamiento esté destinado a los fines policiales legalmente previstos o los datos hayan sido obtenidos de otros ficheros o registros y, en ambos casos, se exima legalmente el cumplimiento de dicho requisito.

5. En la comunicación de datos de carácter personal de ficheros de nivel Alto se aplicará siempre el cifrado de los datos establecido en el artículo 32.5.a DS.

6. Cuando se traten datos de ficheros de nivel Alto, será nulo el consentimiento para la comunicación de los datos de carácter personal a terceros, cuando la información que se facilite al titular o afectado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

7. Excepcionalmente, no se requiere del consentimiento expreso del afectado cuando el tratamiento de los datos resulte indispensable para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria, el tratamiento médico o la gestión de servicios sanitarios, o para salvaguardar el interés vital del afectado (en el supuesto de que el mismo esté física o jurídicamente incapacitado para dar su consentimiento), o de otra persona, siempre que dicho tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por persona supeditada asimismo a una obligación equivalente al secreto.

8. En el ámbito de la salud laboral, el afectado ha de ser informado del destino o uso que se proyecte de la información que se obtenga, de su tratamiento y diagnóstico, que no puede ser otro que la evaluación y vigilancia de la salud de los trabajadores, a los solos efectos de poder identificar cualquier relación entre la causa de la enfermedad o de ausencia y los riesgos para la salud que puedan presentarse en los lugares de trabajo. Para estos fines, los datos sólo pueden ser recabados previo consentimiento del trabajador o, en su defecto, previo informe de los representantes de los trabajadores cuando los reconocimientos y pruebas sean imprescindibles para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores y, en ambos casos, de forma que se causen las menores molestias al trabajador y sean proporcionales al riesgo. Los resultados de la vigilancia serán comunicados a los trabajadores afectados (o recabados por éstos en uso de sus derechos de acceso, rectificación y cancelación), no pudiéndose usar con fines discriminatorios ni en perjuicio del trabajador.

9. Se prohíbe toda comunicación de los datos referidos a la Salud del empleado sin consentimiento expreso del interesado, con la sola excepción de la comunicación interna de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollarse correctamente las funciones preventivas. Los informes de aptitud relativos a los riesgos laborales serán comunicados a los empelados afectados y solo podrán ser conocidos por los mandos directamente vinculados con la atribución de funciones para su conocimiento y consideración a tales efectos.

10. El plazo de exposición pública de los anuncios de resoluciones de expedientes sancionadores (infracciones y sanciones) en el Tablón de Edictos Electrónico, será de veinte días naturales.

Transcurrido el cual se les aplicará el procedimiento de cancelación de oficio, en consonancia con el artículo 45.5 DS.

Artículo 30.- Principios y deberes específicos del tratamiento de datos de carácter personal: adecuación, pertinencia, exactitud y finalidad de los datos.

1. La recogida y el tratamiento de los datos de carácter personal se orientará a que los mismos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los servicios municipales velarán para que los datos de carácter personal sean exactos y estén actualizados, efectuando las actuaciones necesarias a tal fin.

3. Las finalidades legítimas que permiten la recogida de datos de carácter personal, sin consentimiento de los titulares, son únicamente las autorizadas por una ley o norma de Derecho Comunitario para el ejercicio de las competencias municipales. En las no autorizadas legalmente, es preceptivo recabar el consentimiento de los interesados tanto en la recogida como para el tratamiento ulterior.

Artículo 31.- Uso de los ficheros de datos de carácter personal.

Los ficheros de datos de carácter personal se destinarán exclusivamente a las finalidades autorizadas en el Decreto de creación, declaradas en el Registro General de la Agencia Española de Protección de Datos. Su aplicación a otra finalidad requerirá la modificación previa de la inscripción, según el artículo 33 DS, o la autorización expresa de la Agencia Española de Protección de Datos que se instará mediante el Gabinete de Seguridad.

Artículo 32.- Niveles de protección de los ficheros de datos de carácter personal.

1. Atendiendo a la naturaleza de la información tratada y la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma, los ficheros de datos de carácter personal se clasifican en los niveles de seguridad Básico, Medio y Alto. Los niveles de seguridad de los ficheros municipales, la estructura de los datos que contienen y las finalidades o usos de los mismos o de los datos, quedarán inscritos en el Registro General de la Agencia Española de Protección de Datos, según lo dispuesto en el artículo siguiente. La relación de los ficheros inscritos, se mantendrá actualizada en el Anexo II conforme al procedimiento establecido en el citado artículo.

2. A los ficheros municipales que contengan datos de carácter personal y no tengan la consideración de nivel superior, les serán aplicables las medidas de seguridad generales siguientes, de nivel Básico:

a. Las obligaciones de los usuarios del SIM contempladas en el artículo 8 DS.

b. El Registro de Incidencias del artículo 42 DS.

c. El Registro de Accesos establecido de los artículos 21 y 22 DS.

d. Las limitaciones de uso de hardware y software establecidas en el artículo 23 DS.

e. Los principios generales y específicos del tratamiento de datos de carácter regulados en los artículos 29 y 30 DS.

f. Los procedimientos, requisitos y límites de la cesión o comunicación de datos de los artículos 39 y 40 DS.

g. Los procedimientos, requisitos y límites del tratamiento de datos por cuenta de terceros del artículo 41 DS.

h. Los procedimientos, requisitos y efectos del ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los artículos 43 a 46 DS.

3. Son ficheros de nivel Medio los que contengan datos relativos a la comisión de infracciones administrativas y los de Hacienda Municipal, así como aquellos que, por su tratamiento conjunto con otros ficheros o datos, permitan obtener una amplia descripción de la personalidad de los afectados o titulares.

4. A los ficheros de nivel de protección Medio les serán aplicables, además de las medidas de nivel Básico y las establecidas en la normativa sectorial de aplicación, los procedimientos de Auditoria Interna del artículo 52 DS. El acceso a los ficheros por personal no municipal, la distribución de datos y la transmisión de los mismos a través de redes de comunicaciones, precisarán de autorización expresa, debiendo quedar constancia de ésta en las dependencias municipales encargadas del tratamiento.

5. A los ficheros que contengan datos concernientes a la ideología, religión, creencias, origen racial, salud, vida sexual, violencia de género y delitos contra la libertad sexual o datos recabados para fines policiales sin consentimiento de las personas afectadas, calificados de nivel Alto, se les aplicarán, además de las medidas de nivel Básico y Medio, las siguientes de dicho nivel:

a. El cifrado de los datos si su tratamiento se realiza mediante soportes o en ordenadores portátiles según los artículos 25.5 y 37 DS.

b. Las Auditorías mensuales preceptivas establecidas del artículo 22.2 DS.

c. Las limitaciones para la implantación de los ficheros en producción y para la concesión de autorizaciones de acceso a los usuarios, contenidas en los apdos. 6 y 9 del presente artículo.

d. Todas las medidas contempladas en el DS y las que resulten de la normativa sobre protección de datos y de las actuaciones de la Agencia Española de Protección de Datos.

6. La implantación en producción de aplicaciones o programas para la gestión de ficheros de datos de carácter personal, exigirá el previo cumplimiento de las medidas de seguridad que correspondan al nivel asignado al fichero en el Registro General de la AEPD. De ser necesaria la inscripción de un nuevo fichero, la implantación se supeditará a la autorización de aquella.

7. En los ficheros o tratamientos de datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, bastará la implantación de las medidas de seguridad de nivel Básico cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

8. También se aplicarán las medidas de seguridad de nivel Básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

9. Sólo podrán acceder al correspondiente fichero de nivel de seguridad Alto los Administradores señalados en el artículo 16 DS y el personal expresamente autorizado por aquellos cuya identidad haya sido comunicada al Gabinete de Seguridad.

Artículo 33.- Creación, modificación y supresión de ficheros automatizados de datos de carácter personal.

La creación, inscripción, modificación o supresión de los ficheros municipales automatizados de datos de carácter personal -salvo los temporales, que se regirán por lo dispuesto en el artículo 34 DS, y los exceptuados de inscripción por los artículos 35 y 36 DS- se ajustará al siguiente procedimiento:

1. El procedimiento se incoará mediante petición razonada de la Jefatura de Unidad correspondiente remitida al Gabinete de Seguridad.

2. Previo informe del Responsable de Seguridad, se dictará Decreto de Alcaldía ordenando, en su caso, la creación e inscripción del fichero en el Registro General de la AEPD, con el siguiente contenido:

a. Denominación y finalidades o usos del fichero.

b. Personas o colectivos sobre los que se obtendrán datos de carácter personal.

c. Procedimiento, medio y soporte de recogida de los datos de carácter personal.

d. Estructura básica de los datos del fichero.

e. Cesiones previstas del fichero o de los datos, si las hubiera, y norma de rango legal en que se fundamente.

f. Nivel de seguridad asignado y, en consonancia con éste, las medidas de seguridad aplicables en tratamiento del fichero.

g. Encargado del fichero o tratamiento, o servicio o unidad administrativa al que se encomiende su gestión, y ante el que podrán ejercitarse los derechos de acceso, rectificación, cancelación y oposición, conforme a los artículos 43 a 46 DS.

Artículo 34.- Ficheros temporales de datos de carácter personal.

1. Es fichero temporal el creado ocasionalmente para el tratamiento de datos de carácter personal en la gestión de expedientes, la emisión de informes o la realización de trámites, cuyo uso previsible no exceda de los cinco meses de duración, haciendo innecesaria su inscripción.

2. Lo dispuesto en el apartado anterior no obsta para que los ficheros temporales de datos de carácter personal cumplan las medidas de seguridad del presente DS según el nivel de protección que les corresponda.

3. Estos ficheros serán suprimidos por el Encargado del tratamiento una vez cumplida su finalidad y antes del transcurso del plazo señalado en el apartado primero anterior. De preverse la superación de dicho plazo, procederá su inscripción conforme al artículo anterior.

Artículo 35.- Ficheros de imágenes o sonidos y ficheros sujetos a régimen especial.

1. Los ficheros de imágenes y/o sonidos obtenidos por videocámaras fijas de vigilancia de edificios municipales, destinados a garantizar la seguridad interior y exterior de los mismos, siempre que los datos no sean objeto de tratamiento, se crearán por Decreto de la Alcaldía, comunicado a la Delegación Provincial del Gobierno para su constancia en el registro correspondiente, y no precisarán inscripción en el Registro General de la AEPD. El plazo máximo de conservación de de los datos de estos ficheros será de quince días, salvo aplicación a la investigación de los delitos, a expedientes administrativos abiertos o para su remisión a Juzgados y Tribunales.

2. De recabarse imágenes y/o sonidos, mediante dispositivos, fijos o móviles, para finalidades distintas a las señaladas en el apartado anterior, a los ficheros resultantes les será aplicable el régimen previsto en la LO 4/1997, de 4 de Agosto, sobre autorización de uso de videocámaras en lugares públicos, precisando los mismos de autorización de la Comisión Provincial de Video-vigilancia y de inscripción conforme al artículo 32 DS. Estos requisitos deberán asimismo cumplirse cuando las imágenes obtenidas en la vigilancia de edificios sean objeto de tratamiento posterior.

3 En todo caso, la petición a la Comisión de Video-vigilancia sólo se cursará cuando la vigilancia no pueda efectuarse por otros medios que no exijan esfuerzos desproporcionados, según Instrucción de la Agencia Española de Protección de Datos 1/2006.

4. El plazo máximo de conservación de las imágenes de los ficheros incluidos en el apartado segundo será de un mes, y los lugares controlados deberán estar rotulados con la siguiente señalización: "LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS. ZONA VIDEOVIGILADA. Órgano ante el que ejercitar los derechos de acceso, rectificación, cancelación y oposición: (señalar órgano)".

5. La Jefatura de la Policía Local asumirá la custodia de las imágenes y sonidos obtenidos por los procedimientos previstos en el apartado 1 del presente artículo, así como la de aquellos ficheros de la misma clase en que así se determine en la resolución de su creación, así como la responsabilidad de su uso, incluida su inutilización o destrucción, y la resolución de las peticiones de acceso o cancelación promovidas por los interesados conforme a los artículos 43 a 46 DS.

6. Los ficheros de imágenes de vigilancia del tráfico rodado están sujetos al mismo régimen que los restantes automatizados sobre creación, inscripción, modificación y supresión, así como a idénticas medidas de seguridad. Las imágenes así obtenidas deberán ser destruidas en el plazo máximo de un mes, salvo su aplicación a la investigación de los delitos, a la tramitación de expedientes administrativos abiertos o para su remisión a Juzgados y Tribunales.

7. Los ficheros del régimen electoral, los que sirvan a fines exclusivamente estadísticos amparados por la legislación estatal o autonómica sobre la función estadística pública, los procedentes de imágenes y sonidos mediante utilización de videocámaras o grabadoras para su posterior tratamiento, los relativos a control de la salud de los trabajadores municipales y los destinados a la investigación del terrorismo y de la delincuencia organizada, se regirán por el presente DS, en lo no contemplado en su normativa específica ni en la LOPD.

8. Los ficheros de materias clasificadas, en su caso, se rigen por la LO 9/1968, de Secretos Oficiales, según lo preceptuado en el artículo 2 LOPD. Estos ficheros, los temporales de investigación de los delitos y los citados en el apartado primero, no precisan inscripción en el Registro General de la AEPD.

Artículo 36- Ficheros de prestación de servicios.

1. Son ficheros municipales de prestación de servicios los del personal que presta servicios al Ayuntamiento de Granada, cualquiera sea su relación jurídica con el mismo, comprensivos únicamente de los siguientes datos de carácter personal: nombre y apellidos, funciones o puestos desempeñados, dirección postal y/o electrónica y núms. de teléfono y fax.

2. Los ficheros de prestación de servicios no están amparados por la normativa de protección de datos de carácter personal, según lo dispuesto en el artículo 2.2 del RD 1720/2007 (RLOPD).

Artículo 37.- Ficheros de datos de carácter personal en portátiles.

Para el tratamiento de datos de carácter personal en ordenadores portátiles, éstos deben estar cifrados.

Artículo 38.- Prohibición de ficheros no automatizados de datos de carácter personal.

Trascurrido el plazo previsto en la LOPD para la inscripción de ficheros no automatizados de datos de carácter personal, y en aras de la consecución de los objetivos de la LAECSP, queda prohibido el tratamiento de datos de carácter personal en ficheros no automatizados.

CAPÍTULO OCHO. CESIÓN DE DATOS DE CARÁCTER PERSONAL

Artículo 39.- Supuestos que legitiman la cesión de datos de carácter personal.

1. Cesión de datos de carácter personal es el tratamiento de datos que supone su revelación a una persona distinta del interesado.

2. Los datos de carácter personal que obren en expedientes o ficheros sólo pueden ser tratados para su cesión a su titular o afectado. El tratamiento y cesión a terceros, inclusive a representante legal, precisa del consentimiento inequívoco y revocable del titular o de quien ejerza la patria potestad, tutela o curatela sobre menores de edad o discapacitados por resolución judicial. En los ficheros de nivel Alto, el consentimiento se manifestará por escrito de forma expresa.

3. De la anterior prevención general sólo quedan exceptuadas las comunicaciones a las Administraciones Públicas para el ejercicio de sus competencias y la consulta de fondos documentales de los Archivos Municipales (General Administrativo e Histórico) en lo que no afecte a la seguridad pública, el honor, la intimidad y la seguridad de las personas, según la normativa sectorial de aplicación.

4. La cesión de datos de carácter personal autorizada en una ley, no precisa consentimiento de los afectados.

5. La comunicación datos de carácter personal que tenga por destinatarios al Ministerio Fiscal y Juzgados y Tribunales, así como al Defensor del Pueblo y Tribunal y Cámara de Cuentas (u órganos equivalentes de las CCAA), no está sujeta a limitación o condición.

6. La cesión de ficheros elaborados para ejercicio de competencias delegadas, tendrán por exclusivos destinatarios a las Administraciones titulares del fichero o de la competencia, o al órgano especial directamente dependiente de aquellas, y no precisa consentimiento de los afectados. En este epígrafe se encuadran:

a. La comunicación al Instituto Nacional de Estadística y a la Junta de Andalucía de las actualizaciones del Padrón Municipal de Habitantes, conforme a las determinaciones de la LBRL y legislación estatal y autonómica sobre la función estadística pública.

b. La comunicación de datos a la Hacienda Pública.

c. La comunicación de datos a las Fuerzas y Cuerpos de Seguridad para la investigación y persecución de delitos.

d. La comunicación de datos del Impuesto de Bienes Inmuebles al Centro de Gestión Catastral, en aplicación de la legislación en materia de inspección y gestión catastral y tributaria.

7. La comunicación de datos de carácter personal a otras Administraciones para fines históricos, estadísticos o científicos, acreditados en referencia expresa a un proyecto o estudio y/o amparada en la normativa reguladora del ejercicio de los principios constitucionales de colaboración y coordinación, no precisa el consentimiento de los afectados.

8. Tampoco será preciso el consentimiento 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, si bien la comunicación a éstos de los datos sólo será legítima cuando se atenga al cumplimiento de las obligaciones habidas de dicha relación.

9. La cesión de datos de carácter personal a entidades sindicales y asociaciones que se relacionen con el Ayuntamiento de Granada, referidos a los de identificación de los propios afiliados o asociados de la entidad solicitante, de cuyos ficheros, conforme a los artículos 3.d) y 3.g) LOPD, aquellas ostentan la condición de responsables, y el Ayuntamiento la de Encargado del tratamiento, no precisa consentimiento de los afectados.

10. La cesión de datos de los ficheros de prestación de servicios no estará limitada sino por las restricciones, los requisitos y las condiciones que en su caso establezca la Delegación de Personal.

Artículo 40.- Procedimiento de tramitación de expedientes de cesión de datos de carácter personal.

1. En el acto de entrega del dato o datos cedidos, se suscribirá, por el órgano municipal y el cesionario, una comparencia o diligencia en la que se dejará constancia escrita de la fecha y hora, nombre, apellidos y número del funcionario actuante y del cesionario, DNI del cesionario, representación que en su caso ostente el cesionario, norma y/o resolución administrativa en que se fundamente la cesión, datos que se ceden y soporte en que se facilita la cesión con indicación del número de inscripción de éste en el Registro de Soportes de Datos de Carácter Personal. Dicho documento se custodiará en el expediente de su razón en soporte papel o, de existir procedimiento electrónico, en el mismo, previo su escaneado.

2. Las solicitudes de cesión de datos de carácter personal, no comprendidas en los supuestos del artículo anterior, se remitirán al Gabinete de Seguridad CPD y seguirán el siguiente procedimiento:

2.1 El Responsable de Seguridad emitirá informe, previo requerimiento a los solicitantes y, en su caso, de las Áreas o Servicios, de cuantos datos y documentos sean necesarios para fundamentar la resolución, en base a lo prevenido en el artículo 76 de LRJPAC y este DS.

2.2 El expediente se resolverá por Decreto de Alcaldía en el plazo máximo de tres meses, notificándose al interesado y comunicándose a las Áreas o Servicios competentes. La falta de resolución en plazo producirá efectos desestimatorios de la petición, conforme a lo dispuesto en el artículo 42.4 LRJPAC.

2.3 La resolución habrá de pronunciarse sobre los siguientes extremos:

a. La legitimación del peticionario.

b. La aplicación o fichero donde figuren los datos de carácter personal objeto de la cesión.

c. La finalidad y los usos que pretendan darse a los datos interesados, que han de ser compatibles con los declarados del fichero, así como con la naturaleza de los datos y con las medidas y limitaciones legales aplicables según nivel de protección asignado.

d. El procedimiento de abono de las tasas municipales establecidas en la Ordenanza Fiscal correspondiente y de los demás gastos extraordinarios que se devenguen por el tratamiento.

e. Que los datos obren en documentos incorporados a procedimientos finalizados que no sean de naturaleza sancionadora ni disciplinaria.

f. El compromiso de confidencialidad de los cesionarios, que les obliga, por el sólo hecho de la comunicación, a la observancia de los deberes de secreto y custodia de los datos remitidos, por lo que en ningún caso los datos facilitados podrán ser objeto de ulteriores cesiones por parte de aquellos, ni utilizados fuera del estricto ámbito de las relaciones administrativas, profesionales, mercantiles o laborales del cesionario.

g. El procedimiento de disociación aplicado, en su caso, conforme al artículo 29.3 DS.

h. La obligación de cancelar los datos cuando hayan de ser necesarios para la finalidad para la que fueran comunicados.

i. El compromiso expreso del cesionario de atender las peticiones de acceso, rectificación, cancelación y oposición de los afectados sobre los datos comunicados, así como el de observar las disposiciones de la LOPD.

CAPÍTULO NUEVE. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR CUENTA DE TERCEROS

Artículo 41.- Requisitos del tratamiento de datos de carácter personal por cuenta de terceros.

1. El tratamiento de datos de carácter personal por terceros no se considera cesión de datos, pero vincula al Encargado del tratamiento con idéntica responsabilidad que la que legalmente corresponde al

Ayuntamiento en cuanto a finalidad o uso, conservación y destino legítimo de los datos. Por lo que el contratista no podrá destinar los datos a una finalidad distinta de la del objeto del contrato, salvo que, por autorización expresa del Ayuntamiento, deba comunicarlos a un tercero para la prestación de otro servicio, mediante nuevo contrato.

2. El tratamiento de datos de carácter personal por terceros exige la celebración de un contrato de prestación de servicios, en el que ha de contemplarse el cumplimiento de los requisitos y medidas de seguridad señaladas en los apartados 3 a 10 del presente artículo.

3. En todo contrato de prestación de servicios que celebre el Ayuntamiento deberá señalarse su afección o no al tratamiento de datos de carácter personal de los ficheros municipales. En los contratos que no prevean tratamiento de datos de carácter personal, se indicará esta circunstancia, de forma expresa, en el propio contrato, junto con la prohibición de acceso del personal que deba prestarlos a cualquier fichero municipal de datos de carácter personal, amen de la obligación del mismo de guardar estricta confidencialidad, en el supuesto de producirse cualquier acceso incidental, no previsto, a datos de esta naturaleza.

4. De conformidad con lo dispuesto en los artículos 12 LOPD y 82.2 y 88 RLOPD, el contrato de servicios para tratamiento de datos de carácter personal por terceros, que haya de prestarse en locales o dependencias no municipales, deberá describir el fichero o ficheros afectados y recoger el compromiso del contratista de elaborar un Documento de Seguridad que incluya, como mínimo, las medidas de seguridad que se relacionan en Formulario tipo 1del Anexo I DS.

5. Si el contrato implicase tratamiento de datos mediante prestación de servicios en locales y dependencias municipales, el personal a su cargo quedará sujeto al cumplimiento de todas las medidas y procedimientos de seguridad establecidos en el presente DS, y el acceso se limitará exclusivamente al fichero o a los ficheros incluidos en el contrato, según Formulario tipo 2 del Anexo I.

6. Cuando el tratamiento por terceros conlleve el acceso remoto a la red municipal, tanto el contratista como el personal a su cargo quedarán asimismo sujetos, en su integridad, al DS y a las medidas de seguridad del contrato, según Formulario tipo 3 del Anexo I.

7. De los contratos vigentes de prestación de servicios para tratamiento datos de carácter personal por terceros, la identificación del Encargado del tratamiento y su plazo de vigencia, se mantendrá relación actualizada en el Anexo I DS, según lo dispuesto en el artículo 88.5 RLOPD. Para lo que, conforme a lo dispuesto en el artículo 19.3.14 DS, los contratos de servicios que se celebren, así como los convenios que impliquen tratamiento de datos de carácter personal por cuenta de terceros, serán puestos en conocimiento del Gabinete de Seguridad en el plazo de 15 días desde su firma.

8. La subcontratación de servicios contratados para el tratamiento de datos por cuenta de terceros, precisa autorización expresa del Ayuntamiento, salvo previsión de la misma en el contrato inicial, y se concederá para los servicios y ficheros y a favor de la entidad o entidades señalados en el contrato o en la solicitud, obligando al subcontratista en mismos términos y condiciones que al adjudicatario.

9. Si el contratista comunicara los datos de carácter personal sin la autorización municipal, o los aplicara a finalidad distinta del objeto del contrato, podrá acordarse la rescisión de éste y aquel será considerado responsable del tratamiento, respondiendo personalmente de las infracciones en que hubiera incurrido. Esta condición será considerada como obligación contractual esencial en los pliegos de cláusulas administrativas particulares de los contratos que celebren los entes regulados en el artículo 3 DS.

10. De generarse un nuevo vínculo entre quien accede a los datos y los afectados, el tratamiento de datos por tercero deberá tramitarse como cesión o comunicación de datos conforme a lo dispuesto en el artículo 20 del RLOPD.

CAPÍTULO DIEZ. REGISTRO DE INCIDENCIAS

Artículo 42.- Contenido del Registro de Incidencias.

1. Los sucesos acaecidos en el transcurso del tratamiento de datos de carácter personal, que hayan producido o puedan producir algún efecto sobre la integridad y/o seguridad de los mismos, se registrarán en el Registro de Incidencias de datos de carácter personal, mediante la aplicación correspondiente, cuya gestión se asigna al Responsable de Seguridad.

2. En el Registro de Incidencias se inscribirán asimismo los procedimientos realizados de recuperación de los datos, con identificación de la persona que ejecutó el proceso, los datos restaurados y, en su caso, los que haya sido necesario grabar manualmente en el proceso de recuperación.

CAPÍTULO ONCE. ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Artículo 43.- Naturaleza; obligaciones de los órganos municipales y límites.

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos personalísimos de los titulares de los datos, que pueden instarse de forma independiente. El ejercicio de uno de ellos no obstaculizará o afectará a los restantes.

2. La resolución de las peticiones que formulen los interesados en ejercicio de los derechos de acceso, rectificación, cancelación y oposición, es preceptiva, por ser derechos tutelados, amen de en sede judicial, ante la Agencia Española de Protección de Datos, mediante los procedimientos disciplinarios de su competencia. En aplicación de los 17 LOPD y 25.5 RLOPD, sobre la obligación del titular del fichero de conservar la prueba del cumplimiento del deber de respuesta, su satisfacción constituye una obligación jurídica del responsable del fichero o tratamiento, correspondiendo el cumplimiento del deber de respuesta a éste, por lo que el Encargado del tratamiento está obligado a conservar la acreditación de la ejecución de la resolución recaída.

3. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición a datos de carácter personal será gratuito. Las unidades administrativas competentes deberán informar a los afectados de los procedimientos habilitados para el ejercicio de los mismos.

4. El acceso, la rectificación, la cancelación y la oposición, pueden venir referidos a datos de carácter personal obrantes en cualquier expediente administrativo, sobre el sometimiento de los mismos a algún tratamiento, sobre uno o la totalidad de los datos de esta naturaleza incluidos en uno o varios ficheros, acerca de la finalidad del tratamiento, del origen de los datos o de las comunicaciones efectuadas o previstas de aquellos.

5. Los derechos podrán ejercitarse mediante comparecencia personal del interesado o de representante legal o voluntario, siempre que se acredite fehacientemente la representación, dejándose constancia de la misma por cualquier medio válido en derecho, inclusive la comparecencia previa del titular otorgando la representación.

6. Los derechos serán denegados cuando la solicitud se formule por persona distinta del afectado y no se demuestre la representación de aquel. No obstante, en el derecho de acceso, se entenderá acreditada la titularidad o la representación cuando, en relación con los expedientes o los datos a acceder, el solicitante aporte las claves o contraseñas previamente consignadas por la Administración Municipal para este fin.

7. Con carácter general, salvo en el supuesto contemplado en el apartado anterior, y sin perjuicio de los medios de identificación en los procedimientos administrativos en los que se ostente la condición de interesado, las solicitudes contendrán:

a. Nombre y apellidos del titular, fotocopia de su DNI o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

b. Petición en que se concreta la solicitud.

c. Dirección a efectos de notificaciones, fecha y firma del solicitante.

d. Documentos acreditativos de la petición que formula, en su caso.

8. Estos derechos sólo pueden limitarse por razones de Seguridad Pública, en los casos y con el alcance previstos en las leyes.

9. De ejercerse ante el Encargado del tratamiento de un contrato de prestación de servicios, éste remitirá las solicitudes que se formulen al Ayuntamiento en cuanto responsable de aquel, salvo que en el contrato se estipule que el contratista los atenderá por cuenta del Ayuntamiento.

10. Las solicitudes de acceso, rectificación, cancelación y oposición, habrán de resolverse en todo caso, aún cuando no figuren datos personales del afectado en los ficheros municipales.

11. En las solicitudes incompletas o en las que no se acrediten la titularidad o la representación, deberá solicitarse la subsanación de las mismas, requiriéndose, de ser necesario, la concreción o compleción del dato o datos para los que se solicita el acceso, según lo establecido en el artículo 71 LRJPAC.

12. Las reclamaciones que se formulen por denegación o limitación de estos derechos, habrán de ser informadas por el Área o Servicio correspondiente y por el Responsable de Seguridad en el plazo de quince días desde su traslado al Ayuntamiento.

Artículo 44.- Procedimiento y efectos del ejercicio del derecho de acceso a datos de carácter personal.

1. Es acceso a datos de carácter personal la comunicación de éstos a su titular. Este derecho es independiente del acceso a archivos, registros, documentos y expedientes en los que se tenga la condición de interesado conforme a la legislación de procedimiento administrativo.

2. El procedimiento de acceso se caracteriza por su informalidad e inmediatez, ajustándose a la siguiente tramitación:

a. Las solicitudes de acceso se remitirán al Área o Servicio Encargado del tratamiento, que informará sobre de su procedencia o improcedencia.

b. El acceso habrá que concederse o denegarse en el plazo máximo de un mes, comunicándose al peticionario por cualquiera de los medios admisibles en Derecho.

c. De ser procedente el acceso, previa comprobación o constatación de la identidad del solicitante, aquel se hará efectivo en el plazo de los 10 días subsiguientes a la comunicación al interesado, salvo que en ésta se haya aportado la información solicitada. La consulta de datos podrá materializarse en visualización en pantalla, o efectuarse mediante la entrega personal de los datos al interesado o su remisión por fax, copia o fotocopia. Debiendo quedar constancia en el expediente de su razón de su efectiva realización mediante la comparecencia regulada en el artículo 40.1 DS, o por cualquier otro medio que lo acredite, que quedará incorporada al procedimiento (en los procedimientos automatizados, previo escaneado del justificante). El acceso deberá cumplir en todo caso los requisitos del artículo 14 DS.

d. La denegación del acceso requiere tramitación del correspondiente expediente, en la que se dictará resolución mediante Decreto de Alcaldía, que se notificará al peticionario.

e. Dentro de los plazos de prescripción establecidos en el artículo 47 de la LOPD, la resolución denegatoria del acceso será susceptible de reclamación ante la Agencia Española de Protección de Datos

y de la interposición de recurso potestativo de reposición, de lo que se dará cuenta en la notificación remitida.

f. En los ficheros de niveles de seguridad Básico y Medio, la prestación del servicio información por atención telefónica puede hacer necesaria la previa identificación presencial del titular ante el Encargado del tratamiento, para asignación a aquel de una clave o contraseña personales, que le identifique como interlocutor válido en las sucesivas comunicaciones de datos. Este procedimiento será preceptivo para dicho servicio cuando los datos estén contenidos en ficheros de nivel Alto.

3. Además de por no constar los datos solicitados, podrá denegarse el acceso en el supuesto de que, sobre los mismos datos, se haya ejercitado aquel en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

4. Podrá también denegarse el acceso cuando una ley o norma de Derecho Comunitario impida revelar los datos o el tratamiento al que éstos están o han estado sometidos.

Artículo 45.- Procedimiento y efectos del ejercicio de los derechos de rectificación y cancelación.

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. Este derecho podrá ejercitarse en todo momento.

2. La rectificación de datos de carácter personal se aplicará con independencia y sin perjuicio de la revocación y la subsanación de errores materiales de los actos administrativos, establecidos en el artículo 105 LRJPAC.

3. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

4. La cancelación será denegada cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables, o lo impidan obligaciones legales o contractuales.

5. Los datos de carácter personal de carácter disciplinario o sancionador únicamente serán conservados durante el periodo de prescripción de las correspondientes infracciones y sanciones. Transcurrido el mismo, procederá su cancelación de oficio, y en cualquier caso a petición del titular de los datos.

6. La solicitud deberá indicar el dato erróneo o inadecuado, la corrección que deba realizarse o las razones que avalen la cancelación, e ir acompañada de la documentación justificativa, salvo que la

petición venga referida exclusivamente a la revocación del consentimiento del afectado en cuanto a la cesión de datos, en los supuestos en que sea necesario su otorgamiento.

7. El procedimiento se ajustará a la siguiente tramitación:

a. Las solicitudes se remitirán al Área o Servicio Encargado del tratamiento y se resolverán por aquel en el plazo máximo de 10 días desde su recepción por éste.

b. Transcurridos tres meses sin haberse dictado resolución, se entenderá desestimada la petición, a efectos de interposición de la correspondiente reclamación ante la Agencia Española de Protección de Datos (en adelante, AEPD), o de los recursos procedentes, en los plazos establecidos en el artículo 47 de la LOPD.

c. Las resoluciones estimatorias de rectificación y cancelación de datos producirán la activación de un robot TXT o similar que evite la captación de los mismos a través de los buscadores de Internet.

Artículo 46.- Procedimiento y efectos del ejercicio del derecho de oposición.

1. El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal, o a que se cese en el mismo, cuando exista un motivo legítimo y fundado referido a su legítima situación personal, siempre que una ley no disponga lo contrario, o cuando el tratamiento tenga como finalidad evaluar el rendimiento laboral, la solvencia económica o la conducta de aquel, que no corresponda a obligaciones contractuales asumidas.

2. Los efectos de la resolución del reconocimiento del derecho de oposición son los del cese del tratamiento y/o la exclusión en éste de los datos de carácter personal del titular.

3. El procedimiento se ajustará a lo dispuesto en el artículo anterior respecto del ejercicio de los derechos de rectificación y cancelación.

CAPÍTULO DOCE. CERTIFICADOS DE FIRMA ELECTRÓNICA.

Artículo 47.- Oficinas de registro de certificados de Firma Electrónica.

Las Oficinas de Registro de certificados de Firma Electrónica son las constituidas en las Juntas Municipales de Distrito, conforme al Reglamento Municipal de Juntas Municipales de Distrito, dependientes de la Delegación de Participación Ciudadana, así como en las dependencias municipales de los órganos encargados de la gestión del personal y de la coordinación de la información municipal bajo la dirección de la Delegación competente para el desarrollo del sistema conforme al artículo 4 DS. En aplicación del Convenio vigente con la Fábrica Nacional de Moneda y Timbre-RCM y la Junta de Andalucía, la relación de Oficinas de Registro, junto a las IP de las mismas, deberá comunicarse y mantenerse actualizada en el Sistema de Gestión de Oficinas de Acreditación FNMT-RCM por el Gabinete de Seguridad CPD.

Artículo 48.- Registradores de Firma Electrónica.

1. Los registradores de Firma Electrónica estarán adscritos a una de las Oficinas de Registro señaladas en el artículo anterior. En aplicación del Convenio vigente con la Fábrica Nacional de Moneda y Timbre-RCM y la Junta de Andalucía, la relación de registradores de Firma deberá comunicarse y mantenerse actualizada ante las mismas, para cada Oficina, en el Sistema de Gestión de Oficinas de Acreditación FNMT-RCM por el Gabinete de Seguridad CPD.

2. Los registradores Firma Electrónica de las Oficinas de Registro de las Juntas Municipales de Distrito serán propuestos y supervisados por la Dirección General de Participación Ciudadana. Los restantes, por la Dirección General de Personal.

3. Los registradores de Firma Electrónica adscritos a las Oficinas de Registro de las Juntas Municipales de Distrito y al órgano de coordinación de la información, expedirán certificados de Firma Electrónica de la clase C-2 FNMT.

4. Los registradores de Firma Electrónica de Personal de las Administraciones Públicas únicamente expedirán certificados de Firma Electrónica a los empleados municipales. Dichos certificados facultarán para la identificación y la autenticación de los usuarios del SIM en los procedimientos electrónicos implantados en la Sede Electrónica de la Administración Municipal, según lo dispuesto en el artículo 6.1 DS y la Ordenanza Municipal de Administración Electrónica.

Artículo 49.- Procedimientos de expedición, renovación y revocación de Certificados de Firma Electrónica.

Los procedimientos de obtención, renovación y revocación de certificados de Firma Electrónica son los establecidos por la FNMT-RCM en la página web: http://www.cert.fnmt.es/. Los Registradores municipales de Firma Electrónica deberán cumplir taxativamente con dichos procedimientos, especialmente en los trámites de acreditación de la identidad y descarga del Certificado, comunicando al Gabinete de Seguridad las incidencias que se produzcan.

Artículo 50.- Procedimiento de expedición de Certificados de Firma Electrónica a los empleados municipales.

El procedimiento de expedición de Certificados de Firma Electrónica a los empleados municipales será el establecido en la normativa de desarrollo de la Ordenanza Municipal de Administración Electrónica, conforme a su Disposición Adicional Primera.

CAPÍTULO TRECE. AUDITORIAS DEL S.I.M.

Artículo 51.- Auditoria de la Agencia Española de Protección de Datos.

Las medidas, normas y procedimientos de seguridad establecidos en el presente DS están sujetos, en su implantación y ejecución, a las actuaciones inspectoras de la AEPD, en base a lo dispuesto en la LOPD y normativa de desarrollo.

Artículo 52.- Auditorias internas y externas.

1. El SIM será objeto de Auditoria interna con periodicidad, al menos, bianual, así como de las externas que se acuerde celebrar.

2. Los informes de Auditoria dictaminarán sobre la adecuación o pertinencia de las medidas y controles establecidos, señalando las deficiencias en su caso detectadas y proponiendo a la Corporación las medidas correctoras o complementarias a adoptar.

3. Serán objeto de especial atención en los informes de Auditoria:

a. El Registro de Accesos en cuanto a los ficheros de niveles de protección Medio y Alto y la elaboración de los informes correspondientes.

b. El Registro de Incidencias.

c. El Registro de Soportes y los procedimientos de registro, inventariado y custodia de soportes.

d. La inscripción de ficheros de datos de carácter personal.

e. Los procedimientos de tratamiento y cesión de datos de carácter personal.

f. Los trámites de información pública referidos a datos de carácter personal.

g. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos de carácter personal.

h. Los procedimientos de información en línea y de firma electrónica.

i. La seguridad de la red interna (Intranet) del SIM y de su conexión a la externa (Internet).

j. La implantación de las medidas y procedimientos de protección de datos reguladas en el presente Documento y las establecidas en la legislación vigente sobre protección de datos de carácter personal.

k. Los planes de contingencia que deban adoptarse.

DISPOSICIÓN DEROGATORIA

Derogación de la normativa anterior.

El presente DS refunde la normativa sobre Seguridad del SIM anteriormente dictada, a la que deroga. En particular, se declaran derogados el DS aprobado por la Junta de Gobierno Local de 15 de Mayo de 2009 y los dictados por los órganos de dirección de los organismos autónomos municipales.

DISPOSICION FINAL

Aprobación, publicación y entrada en vigor.

El presente documento será aprobado por la Junta de Gobierno Local y entrará en vigor al día siguiente de su íntegra publicación en la Intranet Municipal (Normativa Interna de Seguridad).

ANEXO I. CONTRATOS DE SERVICIOS CON TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL (v. relación de contratos de servicios vigentes en Anexo I. documento aparte)

[Formulario tipo 1: Tratamiento de dd.cc.pp. por cuenta de terceros (artículo 12 LOPD) El encargado tratará los datos en dependencias propias.]

AREA DE _____

Expte.- ……/……

ANEXO AL CONTRATO DE SERVICIOS DE "……." AL AYUNTAMIENTO DE GRANADA.-

Granada,…… de …… de 200__

R E U N I D O S

De una parte,

El AYUNTAMIENTO DE GRANADA representado por D/Dña.. ……, en calidad de Concejal Delegado-a…de ……, …….y ……...

Y de otra parte,

……., domiciliada en _____, C/ _____ provista de C.I.F. nº. _____representada por D/Dña. _____, en calidad de _____ en virtud de los poderes concedidos a su favor mediante escritura pública otorgada ante el Notario D. _____ con fecha _____, bajo el número de protocolo _____.

Ambas partes, reconociéndose previa y recíprocamente la capacidad legal necesaria para el otorgamiento del presente acuerdo

M A N I F I E S T A N

I.- Que, en ejecución de acuerdo de la Junta de Gobierno Local núm. ……y …….., de … de ……. de 200…, ……S.A. es adjudicataria del contrato de servicios "……" y, como consecuencia de la ejecución del mismo, la entidad adjudicataria tiene acceso al/a los fichero(s) "……", de cuyo tratamiento es responsable el Ayuntamiento de Granada, que contiene(n) los siguientes datos de carácter personal de terceros o administrados que mantienen relaciones jurídico-administrativas con el Ayuntamiento:

(Muy importante: describir el contenido del fichero o ficheros objeto del tratamiento)

II.- Que el acceso a estos datos es necesario para el cumplimiento del objeto del mencionado contrato, al que se anexa el presente acuerdo, y que implica el acceso, por personal autorizado de …….. S.A., a los recursos informáticos referidos en apartado anterior.

III.- Por lo que, al objeto de proteger dichos datos de carácter personal y dar cumplimiento a la normativa vigente sobre protección de datos de carácter personal, las partes, puestas libremente de acuerdo, celebran el presente contrato con sujeción a las siguientes:

ESTIPULACIONES

PRIMERA.-

Las partes reconocen que ……. S.A. podrá tener acceso al/a los datos descritos en el apartado I anterior para la prestación de los servicios contratados en cuanto necesarios para el desarrollo de la actividad del Ayuntamiento de Granada. Acceso que se extenderá al tiempo de duración del contrato.

SEGUNDA.-

…….. S.A manifiesta estar al corriente de las obligaciones derivadas de la normativa de protección de datos y, más concretamente, en lo que se refiere a la implantación de las medidas de seguridad previstas en los artículos 82 y ss del RD 1720/2007, de 21 de Diciembre, por el que se aprueba el Documento de desarrollo de la LO 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, todas las cuales se obliga a respetar y cumplir en cuanto Encargado del tratamiento de los ficheros referidos.

TERCERA.-

…… S.A se compromete a tratar los datos únicamente conforme a las instrucciones que reciba expresamente del Ayuntamiento de Granada, a guardar la máxima reserva y secreto sobre la información clasificada como confidencial y a no revelar, transferir, ceder o de otra forma comunicar los mismos a terceros, ya sea verbalmente o por escrito, por medios electrónicos, impresos o mediante acceso informático, ni siquiera para su conservación. A tal efecto, …… S.A sólo permitirá el acceso a los datos de aquellos empleados que tengan la necesidad de conocerlos para la prestación de los servicios contratados.

CUARTA.-

Las medidas de seguridad que …….. S.A se compromete a adoptar para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizados, son las siguientes:

1. Documento de Seguridad: …… S.A elaborará y aprobará un Documento de Seguridad según las determinaciones y contenido establecidos en los artículos 88 y ss del RD 1720/2007.

2. Responsable de Seguridad: …… S.A designará a un Responsable de Seguridad del tratamiento a su cargo durante la prestación de los servicios al Ayuntamiento de Granada, cuya identidad, así como la de quien eventualmente pueda reemplazarle, comunicará puntualmente al Ayuntamiento de Granada.

3. Auditoría: …….S.A realizará una auditoría bianual para comprobar la eficacia de las medidas de seguridad.

4. Funciones y obligaciones del personal: las funciones y obligaciones de cada una de las personas encargadas del tratamiento estarán claramente definidas en el Documento de Seguridad. …….S.A. adoptará las medidas necesarias para que las mismas conozcan las normas de seguridad que afecten al desarrollo de sus funciones, así como las responsabilidades en que pudieran incurrir en caso de incumplimiento.

5. Identificación y autenticación: El mecanismo de identificación y autenticación del personal de ……. S.A será el establecido por el Documento de Seguridad conforme a las instrucciones que en su caso imparta el Ayuntamiento de Granada.

6. Control de acceso físico: …….. S.A dotará de las necesarias medidas de seguridad física a los locales de trabajo donde se ubiquen los equipos de acceso a los ficheros objeto de tratamiento, asegurando el acceso sólo al personal autorizado.

7. Registro de incidencias: ……. S.A dispondrá de un procedimiento de registro de incidencias donde se incluirá la siguiente información: fecha en que se produjo la incidencia, persona que realiza la notificación, persona a quien se comunica, descripción detallada de la incidencia, medidas tomadas para su resolución y fecha de resolución. Cualquier anomalía que se produzca y que afecte o que pudiera llegar a afectar a la seguridad, integridad o confidencialidad de los datos de carácter personal, será inmediatamente notificada al Ayuntamiento de Granada.

8. Gestión de Soportes: El soporte utilizado para la prestación del servicio será el disco duro de los ordenadores personales de los colaboradores designados por …….. S.A para la prestación del servicio. No se realizaran copias de seguridad ni de ningún otro tipo, ni se enviaran para su tratamiento por ningún medio electrónico o físico a ningún lugar, salvo al propio Ayuntamiento de Granada.

QUINTA.-

Las obligaciones establecidas para ……. S.A en las anteriores estipulaciones serán también de obligado cumplimiento para sus empleados y colaboradores (externos e internos), de manera que ……..S.A responderá ante el Ayuntamiento de Granada si tales obligaciones son incumplidas por dichas personas.

SEXTA.-

Finalizada la relación contractual, todos los soportes o documentos que contengan datos de carácter personal objeto del tratamiento serán destruidos o devueltos al Ayuntamiento de Granada.

SÉPTIMA.-

Las obligaciones de confidencialidad establecidas en el presente documento tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre ……..S.A y el Ayuntamiento de Granada.

Y en prueba de conformidad con lo que antecede, ambas partes firman el presente documento, por duplicado ejemplar a un solo efecto, en el lugar y fecha expresados en el encabezamiento.

AYUNTAMIENTO DE GRANADA	(Empresa adjudicataria)
Fdo	Fdo.:
P.P.	P.P.

[Formulario tipo 2: Tratamiento de dd.cc.pp. por cuenta de terceros (artículo 12 LOPD). El encargado tratará los datos con su personal en dependencias municipales.]

AREA DE _____

Expte.- ……/……

ANEXO AL CONTRATO DE SERVICIOS DE "……." AL AYUNTAMIENTO DE GRANADA.-

Granada, …… de …… de 200__

R E U N I D O S

De una parte,

El AYUNTAMIENTO DE GRANADA representado por D/Dña.. ……, en calidad de Concejal Delegado-a…de ……, …….y ……...

Y de otra parte,

……., domiciliada en _____, C/ _____ provista de C.I.F. nº. _____representada por D/Dña. _____, en calidad de _____ en virtud de los poderes concedidos a su favor mediante escritura pública otorgada ante el Notario D. _____ con fecha _____, bajo el número de protocolo _____.

Ambas partes, reconociéndose previa y recíprocamente la capacidad legal necesaria para el otorgamiento del presente acuerdo

M A N I F I E S T A N

I.- Que, en ejecución de acuerdo de la Junta de Gobierno Local núm. ……y …….., de … de ……. de 200…, ……S.A. es adjudicataria del contrato de servicios "……" y, como consecuencia de la ejecución del mismo, la entidad adjudicataria debe acceder al / a los fichero-s "……", "……","……", de cuyo tratamiento es responsable el Ayuntamiento de Granada, que contienen datos de carácter personal de terceros o administrados que mantienen relaciones jurídico-administrativas con el Ayuntamiento.

II.- Que el acceso a estos datos es necesario para el cumplimiento del objeto del mencionado contrato, al que se anexa el presente acuerdo, y que implica el acceso, por personal autorizado de …….. S.A., a los recursos informáticos referidos en apartado anterior.

III.- Por lo que, al objeto de proteger dichos datos de carácter personal y dar cumplimiento a la normativa vigente sobre protección de datos de carácter personal, las partes, puestas libremente de acuerdo, celebran el presente contrato con sujeción a las siguientes:

ESTIPULACIONES

PRIMERA.-

Las partes reconocen que ……. S.A. podrá tener acceso a los citados ficheros, para la prestación del servicio objeto del contrato mencionado, y que este servicio, en cuanto es necesario para el desarrollo de la actividad del Ayuntamiento de Granada, se extenderá al tiempo de duración del contrato. El acceso a referidos ficheros se efectuará mediante el emplazamiento de personal de la empresa adjudicataria en las dependencias municipales del Área de _____. Dicho personal estará permanentemente identificado y autorizado documentalmente tanto por la entidad adjudicataria como por el Ayuntamiento de Granada.

SEGUNDA.-

_____ S.A. manifiesta estar al corriente de las obligaciones derivadas de la normativa de protección de datos y, más concretamente, en lo que se refiere a la implantación de las medidas de seguridad previstas en los artículos 82 y ss del RD 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, así como las contenidas en el Documento de Seguridad del Ayuntamiento de Granada, todas las cuales se obliga a respetar y cumplir en cuanto Encargado del tratamiento de los ficheros referidos. Para lo que cursará las instrucciones precisas al personal a su cargo, al que disciplinará en caso de su incumplimiento, con arreglo a la información e indicaciones del Responsable de Seguridad CPD del Ayuntamiento.

TERCERA.-

_____ S.A. se compromete a tratar los datos únicamente conforme a las instrucciones que reciba expresamente del Ayuntamiento de Granada, a guardar la máxima reserva y secreto sobre la información clasificada como confidencial y a no revelar, transferir, ceder o de otra forma comunicar los mismos a terceros, ya sea verbalmente o por escrito, por medios electrónicos, impresos o mediante acceso informático, ni siquiera para su conservación. A tal efecto, sólo permitirá el acceso a los datos de aquellos empleados que tengan la necesidad de conocerlos para la prestación de los servicios contratados.

CUARTA.-

Finalizada la relación contractual, todos los soportes o documentos que contengan datos de carácter personal objeto del tratamiento serán destruidos o devueltos al Ayuntamiento de Granada.

QUINTA.-

Las obligaciones de confidencialidad establecidas en el presente documento tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre _____ S.A y el Ayuntamiento de Granada.

Y en prueba de conformidad con lo que antecede, ambas partes firman el presente documento, por duplicado ejemplar a un solo efecto, en el lugar y fecha expresados en el encabezamiento.

AYUNTAMIENTO DE GRANADA……..…… S.A

Fdo	Fdo.:
P.P.	P.P.

[Formulario tipo 3: Tratamiento de dd.cc.pp. por cuenta de terceros (artículo 12 LOPD). El encargado tratará los datos con su personal en locales propios, mediante acceso remoto a recursos informáticos municipales.]

AREA DE _____

Expte.- ……/……

ANEXO AL CONTRATO DE SERVICIOS DE "……." AL AYUNTAMIENTO DE GRANADA.-

Granada,…… de …… de 200__

R E U N I D O S

De una parte,

El AYUNTAMIENTO DE GRANADA representado por D/Dña.. ……, en calidad de Concejal Delegado-a…de ……, …….y ……...

Y de otra parte,

……., domiciliada en _____, C/ _____ provista de C.I.F. nº. _____representada por D/Dña. _____, en calidad de _____ en virtud de los poderes concedidos a su favor mediante escritura pública otorgada ante el Notario D. _____ con fecha _____, bajo el número de protocolo _____.

Ambas partes, reconociéndose previa y recíprocamente la capacidad legal necesaria para el otorgamiento del presente acuerdo

M A N I F I E S T A N

I.- Que, en ejecución de acuerdo de la Junta de Gobierno Local núm. ……y …….., de … de ……. de 200…, ……S.A. es adjudicataria del contrato de servicios "……" y, como consecuencia de la ejecución del mismo, la entidad adjudicataria debe acceder al / a los fichero-s "……", "……","……", de cuyo tratamiento es responsable el Ayuntamiento de Granada, que contienen datos de carácter personal de terceros o administrados que mantienen relaciones jurídico-administrativas con el Ayuntamiento.

II.- Que el acceso a estos datos es necesario para el cumplimiento del objeto del mencionado contrato, al que se anexa el presente acuerdo, y que implica el acceso, por personal autorizado de …….. S.A., a los recursos informáticos referidos en apartado anterior.

III.- Por lo que, al objeto de proteger dichos datos de carácter personal y dar cumplimiento a la normativa vigente sobre protección de datos de carácter personal, las partes, puestas libremente de acuerdo, celebran el presente contrato con sujeción a las siguientes:

ESTIPULACIONES

PRIMERA.-

Las partes reconocen que ……. S.A. podrá tener acceso a los citados ficheros, para la prestación del servicio objeto del contrato mencionado, y que este servicio, en cuanto es necesario para el desarrollo de la actividad del Ayuntamiento de Granada, se extenderá al tiempo de duración del contrato. El acceso a referidos ficheros se efectuará mediante personal de la empresa adjudicataria en sus propias dependencias. Dicho personal estará permanentemente identificado y autorizado documentalmente tanto por la entidad adjudicataria como por el Ayuntamiento de Granada.

SEGUNDA.-

_____ S.A. manifiesta estar al corriente de las obligaciones derivadas de la normativa de protección de datos y, más concretamente, en lo que se refiere a la implantación de las medidas de seguridad previstas en los artículos 82 y ss del RD 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, así como las contenidas en el Documento de Seguridad del Ayuntamiento de Granada, todas las cuales se obliga a respetar y cumplir en cuanto Encargado del tratamiento de los ficheros referidos. Para lo que cursará las instrucciones precisas al personal a su cargo, al que disciplinará en caso de su incumplimiento, con arreglo a la información e indicaciones del Responsable de Seguridad CPD del Ayuntamiento.

TERCERA.-

_____ S.A. se compromete a tratar los datos únicamente conforme a las instrucciones que reciba expresamente del Ayuntamiento de Granada, a guardar la máxima reserva y secreto sobre la información clasificada como confidencial y a no revelar, transferir, ceder o de otra forma comunicar los mismos a terceros, ya sea verbalmente o por escrito, por medios electrónicos, impresos o mediante acceso informático, ni siquiera para su conservación. A tal efecto, sólo permitirá el acceso a los datos de aquellos empleados que tengan la necesidad de conocerlos para la prestación de los servicios contratados.

CUARTA.-

El acceso remoto de _____SA a los datos de referido fichero a través de la red de telecomunicaciones se realizará de forma cifrada mediante la funcionalidad que aporte la herramienta de comunicaciones y control remoto elegida por el Ayuntamiento de Granada. A tal fin, el servidor o servidores de conexión deberán necesariamente ubicarse en el Área restringida del centro de tratamiento donde se ubique la Sala de Máquinas del Centro de Proceso de Datos del Ayuntamiento. Su mantenimiento será siempre controlado y dirigido por personal del Centro de Proceso de Datos. La configuración del PC o Nodo de acceso deberá hacerse mediante el servicio de tunelación -modo IPSec de transporte o tunel-

establecido por el Ayuntamiento. Y deberá justificarse en documento anexo el cumplimiento de los siguientes requisitos:

1) Descripción de las características técnicas del servidor o servidores de conexión.

2) El sistema operativo a emplear, que deberá ser original y actualizado.

3) El software de antivirus y el FIRE-walls que incorporará.

4) Los puertos y servicios que deban estar abiertos y/o cerrados para efectuar la conexión.

QUINTA.-

El modo IPSec (transporte o túnel) empleado en cada conexión, garantizará el cumplimiento de las siguientes determinaciones:

A) Autenticidad: Los requerimientos de autenticación de la identidad de los usuarios de la entidad contratada serán establecidos por el Ayuntamiento de Granada, y consistirán, como mínimo, en la asignación del identificador de usuario y la clave privada, únicos para cada usuario, que se facilitarán exclusivamente y de forma segura al representante de misma, Encargado del tratamiento. Dichos requerimientos mínimos podrán ser completados o sustituidos con el certificado digital, a criterio de los servicios técnicos del Ayuntamiento. Los usuarios de la entidad estarán permanente identificados ante el Gabinete de Seguridad CPD del Ayuntamiento.

B) Acceso limitado: Los accesos a los recursos del SIM se limitarán a los necesarios para el cumplimiento del objeto del contrato respecto a los usuarios autenticados.

C) Integridad: Se garantiza que los datos transmitidos por el canal o medio de comunicación no sufrirán alteración, pérdida o manipulación, mediante las funciones *hash criptograficas* de la familia Algoritmo de *hash seguro*.

D) Confidencialidad: Se garantiza que los datos transmitidos por el canal o medio de comunicación sólo serán accesibles para el destinatario de los mismos mediante el esquema de cifrado por bloques AES (Advanced Encryption Standard).

SEXTA.-

_____S.A. (_____) no podrá, bajo ningún pretexto, ejecutar la prestación de servicios objeto del contrato mediante ningún otro programa o aplicación ajeno a la aplicación corporativa facilitada por el Ayuntamiento, ni incorporar los datos del fichero de acceso a ningún otro sistema, soporte o tratamiento distinto de los ya establecidos para aquel por el Ayuntamiento de Granada, titular del fichero.

SÉPTIMA.-

Finalizada la relación contractual, todos los soportes o documentos que contengan datos de carácter personal objeto del tratamiento serán destruidos o devueltos al Ayuntamiento de Granada.

OCTAVA.-

Las obligaciones de confidencialidad establecidas en el presente documento tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre _____ S.A y el Ayuntamiento de Granada.

Y en prueba de conformidad con lo que antecede, ambas partes firman el presente documento, por duplicado ejemplar a un solo efecto, en el lugar y fecha expresados en el encabezamiento.

AYUNTAMIENTO DE GRANADA……..…… S.A

Fdo

P.P.

Fdo.:

P.P.

ANEXO II. FICHEROS DE DATOS DE CARÁCTER PERSONAL INSCRITOS EN REGISTRO GENERAL AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS / NIVELES DE SEGURIDAD, CÓDIGOS DE INSCRIPCIÓN Y USOS (v. relación de ficheros inscritos en AEPD en Anexo II -documento aparte)

ANEXO III. DEFINICIONES, TÉRMINOS Y CONCEPTOS

Acceso autorizado	Autorización concedida a un usuario para la utilización de un recurso informático
Administrador	Superusuario-a con funciones de alta, baja y asignación de niveles de perfil en uno o varios ficheros respecto a otros usuarios, bajo la supervisión del Responsable de Seguridad
Aplicación	Conjunto de programas y procedimientos que permiten el acceso a los ficheros o bases de datos
Asignación de perfil	Procedimiento de concesión de capacidades de acceso a los usuarios según niveles y escalas descritos en anexos IV a VI. Solo puede definir perfiles a otros usuarios un superusuario
Asignación de privilegios	Procedimiento que permite conceder privilegios a un usuario en una determinada aplicación, y en los trámites y utilidades que se especifiquen, con el tipo de competencia que se establezca para cada operación
Auditoria AEPD	La que, en base a la legislación vigente, corresponde a la Agencia Española de Protección de Datos sobre las medidas y normas de seguridad del SIM
Auditoria del Registro de Accesos	Informe de los accesos de los usuarios a los ficheros (de periodicidad mensual para los ficheros de nivel Alto u ocasional para los de niveles Medio y Básico) que realiza el Responsable de Seguridad mediante el Registro de Accesos
Auditoria externa	Dictamen sobre cumplimiento de las medidas y normas de seguridad adoptadas y resumen de las conclusiones y necesidades detectadas, que eleva a la Corporación la entidad de Seguridad Informática que al efecto se contrate
Auditoria interna	Dictamen, de periodicidad al menos bianual, sobre cumplimiento de las medidas y normas de seguridad establecidas y resumen de las conclusiones y necesidades detectadas, que eleva a la Corporación el Responsable de Seguridad
Autenticación	Procedimiento de comprobación de la identidad del usuario
Autorización de acceso	Permiso del usuario para acceder o tratar ficheros o aplicaciones de datos de carácter personal y utilizar cualesquiera recursos informáticos, según procedimientos de identificación y autenticación regulados en el presente DS
Caducidad	Fecha (actualizable) a partir de la cual quedan revocados los privilegios asignados al usuario
Centro de Proceso de Datos (CPD)	Dependencia municipal donde se traten automatizadamente datos. Los centros de tratamiento del CPD se distribuyen en tres grupos de áreas: 1) Áreas abiertas: dependencias municipales donde se ubican los equipos informáticos destinados a la prestación de servicios

	municipales 2)Áreas limitadas: dependencias municipales antesalas de las áreas controladas y/o que almacenan soportes informáticos 3) Áreas controladas: dependencias donde se ubican los equipos centrales del SIM (Centro de Proceso de Datos: CPD). Se subdividen en: 3.a) Área restringida: recinto donde se encuentran los equipos centrales, servidores y comunicaciones. 3.b) Áreas internas: resto de zonas del C.P.D. donde habitualmente presta servicio el personal adscrito al mismo, sin incluir el área limitada
Cesión de datos de carácter personal	Tratamiento de datos de carácter personal orientado a su revelación a persona distinta del titular para los supuestos y fines expresamente autorizados
Competencia de Consulta	Privilegio que permite consultar el documento generado en el trámite para el que se asigna
Competencia de Ejecución	Privilegio que permite la realización y modificación del trámite o utilidad para el que se asigna
Contraseña	Información confidencial, constituida por una cadena de caracteres, que identifica y autentica a un usuario
Control de accesos de usuarios	Procedimiento de comprobación de los accesos de los usuarios asentados en el Registros de Accesos
Copia de respaldo (backup)	Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación
Custodia de soportes	Operación de almacenamiento, registro, control de entrada y salida, emplazamiento y acceso de/a los soportes informáticos del Área o Servicio

Datos de carácter personal	Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión por cualquier medio, concerniente a una persona física identificada o identificable. A los citados efectos, son datos de carácter personal: 1) Los nominativos: nombre y apellidos, D.N.I., N.I.F., (tratándose de extranjeros, el documento que lo sustituya), teléfono, cuentas corrientes, e-mail, etc. 2) Los concernientes a la vida personal y familiar: domicilio, nacionalidad, lugar y fecha de nacimiento, nivel de estudios, ingresos, gastos, aficiones, propiedades, hijos, nivel formativo, trabajo, etc. 3) Los que hagan referencia a ideología, origen racial, salud, religión o creencias, vida sexual, afiliación sindical/política, etc.[2] 4) Las imágenes y sonidos grabados por cualquier medio técnico que permita su reproducción
Disociación	Procedimiento de fragmentación y/o generalización de datos de carácter personal que, aplicado a la cesión de los mismos, imposibilitará la identificación del titular en ulterior tratamiento
Documento	Pieza mínima de información automatizada con significado propio
Encargado del fichero o tratamiento	Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos de carácter personal por cuenta del responsable del tratamiento
Equipo	Elemento de hardware de gestión del SIM. Son equipos centrales: Mainframe, Mini, Servidores y sus componentes. Son equipos periféricos: los ordenadores personales y sus componentes
Escala de asignación de perfil	Relación gradual de las facultades de acceso y niveles de reserva de los usuarios sobre los dossieres. Cada perfil se define para un tipo de expediente, salvo el de superusuario, que es válido para todos los tipos. La escala de asignación de perfiles se representa en tabla incluida en anexo V
Estado (de tramitación)	Hito procesal del que depende la operatoria futura de un dossier
Fichero	Conjunto de registros, subdividido en campos, que contienen o pueden contener datos

2 En definición legal, “especialmente protegidos” (artículo 7 LOPD).

Fichero automatizado de datos de carácter personal	Conjunto informatizado de datos de carácter personal. En consonancia con la importancia de los datos que contienen y las medidas de seguridad adoptadas para su custodia, se clasifican en: c.1) De nivel Básico. c.2) De nivel Medio. c.1) De nivel Alto.
Firma electrónica	Conjunto de datos, en forma electrónica, consignados junto a otros datos electrónicos o asociados con ellos, que pueden ser utilizados como medio para identificar al firmante
Identificación	Procedimiento de reconocimiento de la identidad de un usuario o soporte informático
Incidencia de datos de carácter personal	Cualquier suceso acaecido en el tratamiento de datos de carácter personal (ficheros y/o soportes) del que haya derivado o pueda originarse alguna consecuencia sobre la seguridad del SIM y/o la integridad y confidencialidad de los datos, cuya comunicación al Gabinete de Seguridad es preceptiva por parte del Encargado del tratamiento para su constancia y tramitación por el Registro de Incidencias
Informe de Seguridad	Dictamen del Responsable de Seguridad sobre aplicación de las medidas, normas y procedimientos de seguridad y Auditorías del Registro de accesos
Inscripción	Procedimiento obligatorio de alta, baja o modificación de ficheros de datos de carácter personal en el Registro General de la Agencia de Protección conforme a Decreto de Alcaldía (de soportes en el Registro de soportes)
Medios, procedimientos y medidas de seguridad	Las implantadas en el presente DS y disposiciones de desarrollo para evitar la alteración, pérdida, tratamiento, comunicación o acceso no autorizados de datos de carácter personal
Modificación de la fecha de caducidad	Procedimiento que permite alterar la fecha de vigencia de privilegios
Operación	Cualquier actuación que modifica un dossier añadiendo un documento, actualizando su ficha o cambiando su estado. Las operaciones en el S.I.M. pueden ser de dos tipos: trámites y utilidades. Por lo que respecta a los trámites, se distingue entre competencia de consulta y de ejecución. En el caso de las utilidades solo está habilitada la competencia de ejecución. Dichas competencias tienen una vigencia determinada por la fecha de caducidad que se especifique
Perfil	Autoridad vertical concedida a un usuario y que define su capacidad para acceder a dossieres y los niveles de reserva que puede asignarles (v. reglas y escala de niveles en anexos IV y V).
Privilegio	Facultad que autoriza a un usuario para efectuar consultas o trámites a nivel de aplicación, carpeta o fichero o a nivel de dossier
Programa	Cualquiera de los elementos de software que sirve de base al S.I.M. para tratamiento de ficheros

Propietario	Es el creador inicial de un dossier. Es posible modificarlo
Recurso informático	Partes o componente del SIM sin descripción específica
Redes abiertas de telecomunicación	Infraestructura de telecomunicación libremente accesible por cualquier usuario de los servicios que permiten la transmisión e intercambio de datos y el acceso a la información disponible en Internet mediante su conexión a medios informáticos
Registro de Accesos	Aplicación de anotación y tratamiento de los accesos al SIM de los usuarios de la Administración Municipal
Registro de Incidencias	Aplicación del programa de comunicaciones internas para anotación y tratamiento de las comunicaciones de incidencias de datos de carácter personal
Registro de Soportes	Aplicación de anotación de los datos de identificación y de las operaciones de entrada y salida de la Administración Municipal de los soportes de datos de carácter personal y del contenido de éstos
Responsable de Seguridad	Persona a la que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables
Responsable del fichero o tratamiento	A efectos del presente DS, el Ayuntamiento de Granada como persona jurídico-pública que decide sobre la finalidad, contenido y uso del tratamiento
Revocación de privilegios	Procedimiento que permite anular todas las competencias previamente concedidas a un usuario en una aplicación
Servidor de ficheros	Elemento de hardware que, mediante el software correspondiente, permite el almacenamiento centralizado y el tratamiento compartido de información entre ordenadores periféricos
Sistema de Información Municipal (SIM)	Conjunto integrado de centros de tratamiento, locales, equipos y aplicaciones, así como de personas, dependientes del Ayuntamiento de Granada, que intervienen en el almacenamiento y tratamiento automatizado de datos. Son componentes del SIM, los siguientes: 1) El Servicio de Información Municipal (SIM): conjunto de procedimientos, programas y personal especializado encargado de la gestión y mantenimiento de las aplicaciones corporativas. 2) El Servicio de Gestión de Expedientes (TELNET): conjunto de programas y personal encargado de la gestión y mantenimiento de los procedimientos administrativos (son bases de datos corporativas). 3) Red interna (Intranet) y Servicio de Información Geográfica: Estructura organizada de ordenadores, software, información geográfica y personal especializado para solucionar eficientemente la captura, almacenamiento, actualización, manipulación, análisis y presentación de todo tipo de información referenciada geográficamente

Soporte informático	Disco magnético u óptico u objeto físico susceptible de ser tratado en el SIM o en otro sistema informático y mediante el que se puedan grabar, comunicar y recuperar datos
Titular o afectado	Persona física a la que vienen referidos datos de carácter personal de cualquier fichero o tratamiento del SIM
Trámite	Operación que modifica un expediente administrativo informatizado
Tratamiento	Cualquier operación o procedimientos técnico, automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación o supresión, así como las cesiones de datos que resulten de las comunicaciones, consultas, interconexiones y transferencias de datos de carácter personal
Uso del fichero/aplicación	Finalidad del tratamiento acorde con la declarada en la disposición de creación del fichero
Usuario	Sujeto de la Administración Municipal autorizado para el acceso a o el tratamiento de datos o recursos del SIM
Utilidad	Operación que realiza explotaciones sobre los datos asociados a una aplicación. También permite la modificación masiva de dossieres mediante la ejecución repetida de uno o varios trámites sobre los mismos

ANEXO IV. REGLAS DE ASIGNACIÓN DE PERFILES

Perfil	Acceso	Acciones posibles
Superusuario	Todos, todos los tipos.	Todas
Usuario privilegiado	Todos, un tipo.	Todas, un tipo.
Confidencial	Confidenciales y acceso restringido de su propiedad.	Cambio de reserva dossier hasta acceso restringido.
Reservado	Reservados.	Cambio de reserva dossier hasta reservado.
Datos personales	Datos personales.	Cambio de reserva hasta datos personales.
Dominio público	Dominio público	Cambio reserva hasta dominio público.
Sin autorización	Sin protección	Ninguna.

ANEXO V. ESCALA DE ASIGNACIÓN DE PERFILES

Superusuario: Tiene acceso a todos los niveles de reserva.
Usuario privilegiado: Tiene todas las autorizaciones en un tipo de expediente.
Confidencial: Accede a información catalogada como tal y con acceso restringido siempre que sea su propietario.
Reservado: Accede a los niveles de reserva iguales o inferiores al nivel de reserva denominado información reservada.
Datos personales: Accede a los niveles de reserva iguales o inferiores al nivel de reserva denominado información de carácter personal.
Dominio público: Accede a los niveles de reserva iguales o inferiores al nivel de reserva denominado dominio público.
Sin autorización: Accede solo a información no protegida.

ANEXO VI. ESCALA DE NIVELES DE RESERVA

Acceso restringido: Acceso permitido únicamente a propietario y usuario con acceso restringido.
Confidencial
Información reservada
Información de carácter personal
Dominio público
Sin protección.

ANEXO VII. PROCEDIMIENTOS DE GESTIÓN DE COPIAS DE RESPALDO (BACK-UPS)

(Procedimientos sujetos a modificación por razones técnicas)

- Back-up completo de la Red Novell: semanal, hasta completar cinco semanas consecutivas.

- Back-up completo de la Red Novell: de dos semanas completas.

- Back-up completo del Archivo Histórico y servidor del Servicio Contraincendios y Protección Civil: de dos semanas completas.

- Back-up completo del Ordenador Central (Host): uno diario de hasta dos semanas completas.

- Back-up completo de todo el S.O: uno diario de hasta dos semanas completas; más uno semanal y uno mensual. Custodia de las cintas por los mismos plazos y, respecto al mensual, durante 24 meses consecutivos.