Administración Local

Ayuntamientos

CAMPONARAYA

ANUNCIO DE APROBACIÓN DEFINITIVA DEL REGLAMENTO MUNICIPAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DEL AYUNTAMIENTO DE CAMPONARAYA

Al no haberse presentado reclamaciones durante el plazo de exposición al público, queda automáticamente elevado a definitivo el acuerdo plenario inicial aprobatorio de la Ordenanza municipal reguladora del Reglamento municipal de protección de datos de carácter personal del Ayuntamiento de Camponaraya, cuyo texto íntegro se hace público, para su general conocimiento y en cumplimiento de lo dispuesto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

«REGLAMENTO MUNICIPAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, prevé que las funciones y obligaciones del personal en materia de protección de datos, se encuentren detalladas en el Documento de Seguridad, como así se recoge en el artículo 89.

El Ayuntamiento de Camponaraya es responsable de ficheros de datos de carácter personal necesarios para el cumplimiento de las funciones que por ley le son encomendadas como entidad local. La necesidad de proceder a adoptar las medidas de seguridad adecuadas para tales ficheros a la legislación en materia de protección de datos, es motivo de redacción del presente Reglamento.

Artículo 1º. Objeto

El objeto de este Reglamento es la aprobación del documento interno de funciones y obligaciones del personal con acceso a datos de carácter personal contenido en el anexo I.

Artículo 2º. Entrada en vigor

De conformidad con lo dispuesto en los artículos 49 y 65.2 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, el presente Reglamento entrará en vigor una vez transcurrido el plazo de quince días hábiles desde su publicación en el Boletín Oficial de la Provincia.

ANEXO I: OBLIGACIONES QUE AFECTAN A TODO EL PERSONAL

Puestos de trabajo de los usuarios de los ficheros:

Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

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

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

Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el Responsable de Seguridad, quedando constancia de esta modificación en el Registro de Incidencias. Esta prohibición alcanza al uso desde el puesto de trabajo que el Ayuntamiento facilita al trabajador, de programas de intercambio de ficheros (tipo P2P, FTP, partición de discos, o tecnologías análogos o similares), programas de mensajería instantánea, ya sean sobre platafor-

mas web o vía messenger o IRC (así como tecnologías similares o análogas a las mismas). También se prohíbe la conexión de accesorios periféricos no autorizados a los equipos de trabajo, los cuales se detallan en el anexo 1.

Se prohíbe el uso de soportes no autorizados por el Responsable de Seguridad (cds, Vds., memorias, etc…) susceptibles de almacenar información de los ficheros, así como su transmisión por vía electrónica, siendo responsable el trabajador del uso y destino de la misma.

El uso del correo electrónico corporativo queda limitado a su uso profesional. Queda terminantemente prohibida su utilización para el envío y recepción de correos personales.

Cuando un usuario sea dado de baja en el sistema de correo electrónico, el Ayuntamiento podrá libremente decidir si elimina los mensajes y libreta de direcciones guardados en el directorio de correo electrónico de la dirección que causa baja o por el contrario se conservan conforme a la normativa vigente en materia de protección de datos de carácter personal.

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

Si el usuario tuviera indicios de que su ordenador pudiera estar infectado por un virus informático, o cualquier software malicioso, deberá avisar al Responsable de Seguridad.

El usuario debe asegurarse de que la información (datos y programas) contenida en el ordenador no es transferida a ningún soporte físico externo ni a ningún dispositivo conectado al ordenador.

Una vez que el usuario haya finalizado su trabajo, procederá a apagar el ordenador personal y todos sus periféricos, salvo que sea necesario mantenerlo encendido por razones operativas, en cuyo caso deberá cancelar su identificación-autenticación, de conformidad con lo establecido en el anterior apartado.

Aplicaciones:

Las aplicaciones son aquellos sistemas o programas informáticos mediante las cuales se puede acceder a los datos del fichero.

El acceso a las aplicaciones será restringido y su control se realizará mediante un código de usuario y una contraseña asignada a dicho usuario. El código de usuario será único y estará asociado a la contraseña correspondiente que sólo deberá ser conocida por el usuario y que quedará bajo su exclusiva responsabilidad. En caso de que el usuario detecte cualquier anomalía en cuanto al uso de su contraseña deberá comunicar la incidencia correspondiente.

No se utilizaran claves, contraseñas o códigos genéricos.

El control de acceso mediante contraseña y código de usuario podrá ejecutarse directamente desde la aplicación correspondiente o a través del sistema operativo por medio del cual se ejecute la aplicación.

Si durante las pruebas anteriores a la implantación o modificación de acceso al fichero se utilizasen datos reales, se deberá aplicar a dichos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo fichero. En el supuesto de que no se pudiera garantizar dicho nivel de seguridad, no se utilizarán en las pruebas datos reales.

Sistema operativo y de comunicaciones:

Cuando el fichero se encuentre ubicado en un ordenador, al contar este con un sistema operativo determinado y poder contar con unas conexiones que le comuniquen con otros ordenadores, es posible que determinadas personas no autorizadas puedan acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación correspondiente.

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

1.- El sistema operativo y de comunicaciones del fichero deberá tener al menos un responsable, que, como Administrador deberá estar relacionado en el Documento de Seguridad. En el supuesto de no existir el Administrador, sus funciones serán desempeñadas por el Responsable de Seguridad.

2.- En el caso más simple, como es que el fichero se encuentre ubicado en un ordenador personal y sea accedido mediante una aplicación local monopuesto, el Administrador del sistema operativo podrá ser el mismo usuario que acceda usualmente al fichero.

3.- Ninguna herramienta o programa de utilidad que permita el acceso al fichero deberá ser accesible a personas no autorizadas.

4.- Si la aplicación o sistema de acceso al fichero utilizase normalmente ficheros temporales, ficheros de "logging" o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el Administrador deberá asegurarse de que esos datos no son accesibles posteriormente para personal no autorizado.

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

Salvaguarda y protección de las contraseñas personales:

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

Cada usuario del sistema tendrá su propio nombre de usuario para proceder a su identificación y una contraseña ligada a este nombre de usuario para proceder a la autenticación. Ambos serán custodiados con la máxima confidencialidad.

Se establecerá un sistema de asignación de contraseñas que garantice su confidencialidad e integridad, y mientras estén vigentes se almacenarán de forma ininteligible. Las contraseñas contendrán al menos 6 caracteres alfanuméricos y se evitará que se correspondan con nombres de empleados, familiares o cualquier otro que sea de fácil deducción.

Al usuario le será asignada una contraseña de sesión la primera vez que se identifique contra el sistema, debiendo en este acto elegir una nueva contraseña que le acompañará hasta que el responsable de Seguridad decida asignarle una nueva clave de sesión, debiendo el usuario repetir el proceso anterior.

Las contraseñas no se almacenarán de forma legible ni entendible como lo puede ser un papel y cambiarán de forma que no se repitan al menos durante cuatro meses.

Obligación de secreto:

Todos los usuarios están obligados a mantener estricto secreto profesional y rigurosa confidencialidad respecto de cualesquiera datos y recursos a los que tengan acceso en el desarrollo de sus tareas y funciones. Esta obligación se mantendrá aun en el caso de extinción de la relación que vinculen a las partes.

Por tanto, y sin perjuicio de las excepciones legalmente establecidas, se prohíbe categóricamente facilitar datos de carácter personal a cualquier persona que no sea titular de los mismos, salvo que esta acredite encontrarse debidamente autorizada por el titular para recabar y obtener información sobre los mismos. Dicha prohibición habrá de observarse incluso cuando la persona solicitante de la información acredite relación familiar, por próxima que esta sea, con la persona a la que los datos conciernan.

Si un usuario recibe visitas en su puesto de trabajo, cuidará especialmente de que la información utilizada, tanto en pantalla como impresa (por ejemplo, listados), quede fuera del alcance visual del visitante.

Esta obligación de secreto se hará extensible a la revelación de datos de carácter personal, no sólo de forma verbal sino también mediante la revelación, entrega, reproducción o cualquier otro medio físico de transmisión de datos.

Comunicación de las incidencias:

Si el usuario tuviera indicios de que su ordenador pudiera estar infectado por un virus informático deberá avisar al Responsable de Seguridad.

Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal habrá de ser inmediatamente comunicada por el usuario que la detecte al Responsable de Seguridad, el cual mantendrá y gestionará el registro de todas las incidencias que se produzcan, en cumplimiento de lo establecido en los artículos 90 y 100 del Reglamento.

Cualquier usuario que tenga conocimiento de una incidencia es responsable de la comunicación de la misma al administrador del sistema, o en su caso, del registro de la misma en el sistema de Registro de Incidencias del fichero.

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

Cumplimiento del deber de información:

Si en algún momento cualquier usuario fuese requerido para facilitar el ejercicio de los derechos que la LOPD confiere a los titulares de datos personales, deberá indicarle que se ponga en contacto con el número de teléfono principal del Ayuntamiento en recepción o secretaría.

Desde los puestos de recepción o secretaría se informará al interesado que puede ejercer sus derechos de la siguiente manera:

* Dirigir comunicación por carta o fax al Responsable del fichero, que proceda en su caso.
* Fotocopia del DNI.
* Especificación del derecho que desea ejercer

Todas las comunicaciones que se reciban se pondrán en conocimiento del Responsable de Seguridad quien las hará llegar al Responsable del fichero.

El derecho de acceso podrá ser atendido mediante el visionado en pantalla, después de haber rellenado el formulario predispuesto para tal fin.

Procedimiento de gestión de documentación en soporte papel

Fases de aplicación:

El procedimiento de gestión se aplicará en todas las fases de tratamiento de la información en soporte papel que contenga datos de carácter personal. Se identifican las siguientes fases:

a. Archivo
b. Destrucción
c. Confidencialidad

a) Archivo

En esta fase, el personal autorizado seguirá los siguientes pasos:

- Clasificación de la información recibida
- Apertura de un expediente
- Asignación al expediente de un código alfanumérico progresivo

Estas tareas se realizarán de acuerdo con las instrucciones facilitadas por los superiores de departamento y conforme al sistema de archivo del Ayuntamiento.

En los traslados de los expedientes, se guardarán todas las medidas de seguridad apropiadas, teniendo en cuenta la importancia de la información en ellos contenida, el estado de la técnica y la diligencia profesional debida.

La documentación en papel será almacenada en archivos, armarios etc... con llave y sólo los usuarios autorizados podrán tener la llave de apertura de los mismos.

La información consultada y utilizada en las tareas administrativas deberá ser devuelta al finalizar la jornada de trabajo a su lugar cerrando con llave de nuevo la dependencia dónde se ubique. De igual modo se procederá cuando el usuario abandone su puesto durante un período largo, no debiendo quedar documentación sensible en su lugar de trabajo.

B) Destrucción

La destrucción de la documentación que contenga información de carácter sensible se realizará mediante el uso de las máquinas destructoras de papel.

c) Confidencialidad

El trabajador tiene prohibido sacar de las instalaciones del Ayuntamiento documentación que contenga información del Ayuntamiento, así como cualquier otra información que contenga datos de clientes, proveedores o empleados.

ANEXO 1: ACCESORIOS PERIFÉRICOS NO AUTORIZADOS

1. Unidades de CD o DVD grabables o regrabables
2. Unidades de memoria flash
3. Unidades de memoria usb
4. Discos duros externos
5. Unidades reproductoras de sonido, imagen, a titulo enunciativo se mencionan las unidades tipo mp3 o mp4 susceptibles de almacenar datos
6. PDAS y teléfonos móviles, ya sea mediante cable o vía bluethooth o infrarrojos

7. Unidades de disquete»

Contra el presente acuerdo, se interpondrá recurso contencioso-administrativo, ante la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia, en el plazo de dos meses a contar desde el día siguiente a la publicación del presente anuncio, de conformidad con el artículo 46 de la Ley 29/1998, de 13 de julio, de la Jurisdicción Contencioso-Administrativa.

En Camponaraya, a 31 de marzo de 2014.–El Alcalde, Fernando López Rellán.

3209