Obligaciones de los usuarios del Sistema de Información Municipal del Ayuntamiento de Granada

Según establece el vigente Documento de Seguridad Municipal aprobado por Junta de Gobierno Local el 20 de abril de 2012

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.