SESIÓN ORDINARIA CELEBRADA POR LA JUNTA DE GOBIERNO LOCAL EL DÍA VEINTICUATRO DE MAYO DE DOS MIL DIECIOCHO.

En la ciudad de Granada y en la Sala de Reuniones de Alcaldía del Palacio Consistorial, siendo las trece horas y treinta minutos del día veinticuatro de mayo de dos mil dieciocho, bajo la Presidencia del Ilmo. Sr. Teniente de Alcalde Don Baldomero Oliver León, se reúnen los miembros de la Junta de Gobierno Local: los Concejales y Concejalas Doña Raquel Ruz Peis quien actúa como Concejala-Secretaria al amparo de lo dispuesto en el artículo 17.4 del Reglamento Orgánico Municipal, Don Miguel Ángel Fernández Madrid, Doña Jemima Sánchez Iborra y Doña María de Leyva Campaña.

No asisten con excusa el Sr. Alcalde-Presidente, Don Francisco Cuenca Rodríguez, la Sra. Teniente de Alcalde Dª Ana Muñoz Arquelladas y el Sr. Concejal Don Eduardo José Castillo Jiménez.

Asimismo asisten Don Ildefonso Cobo Navarrete, Secretario General y el Interventor Don Francisco de Paula Aguilera González, que asiste a los solos efectos de posibles consultas sobre los expedientes ya fiscalizados, con el fin de celebrar la presente sesión ordinaria para la que previamente han sido citados.

Abierta la sesión por la Presidencia se pasan a tratar los siguientes puntos del Orden del Día:

570

Aprobación de la normativa de seguridad: Creación y uso de contraseñas en el Ayuntamiento de Granada.

Visto expediente **núm. 154/2018** del Centro de Proceso de Datos, relativo a la **Aprobación de la normativa de seguridad: Creación y uso de contraseñas en el Ayuntamiento de Granada.**

Visto el informe de fecha 13 de abril de 2018, emitido por el Subdirector de Seguridad, que lleva la firma del Director Técnico del Centro de Proceso de Datos y el conforme del Coordinador General de Economía, Personal, Contratación y Smart City, en relación a la aprobación de la normativa de seguridad: “Creación y uso de constraseñas en el Ayuntamiento de Granada”, del siguiente tenor literal:

“NORMATIVA DE SEGURIDAD: “CREACIÓN Y USO DE CONTRASEÑAS EN EL AYUNTAMIENTO DE GRANADA”

INTRODUCCIÓN

Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos siendo la primera línea de protección para las personas usuarias. Una contraseña mal elegida o desprotegida puede resultar en una amenaza de seguridad para toda la organización. Por ello, todas las personas usuarias de la red corporativa del Ayuntamiento de Granada son responsables de velar por la seguridad de las contraseñas seleccionadas por ellas mismas para el uso de los distintos servicios informáticos municipales.

En particular, el tratamiento de la información en el Ayuntamiento de Granada requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la pareja de credenciales: usuario y contraseña. Por la seguridad de los servicios y sistemas en los que existen cuentas de usuarios, se ha de garantizar que las credenciales de autenticación se generan, actualizan y revocan de forma óptima y segura.

REGULACIONES INTERNAS DE SEGURIDAD EN EL SECTOR PÚBLICO

Las entidades del Sector Público, en el desarrollo de sus funciones de servicio, policía o fomento, están sometidas a diferentes normativas, de carácter europeo, estatal, autonómico o local. En concreto, la particularidad de la actuación administrativa realizada por medios electrónicos viene requiriendo, la existencia de normas asimismo específicas, al objeto de acomodar aquellas funciones originarias a los condicionantes y medios electrónicos.

En este sentido, la ya derogada Ley 11/2007 supuso el punto de partida de un extenso compendio de regulaciones que vienen completando nuestro moderno ordenamiento jurídico administrativo-electrónico, entre las que cabe destacar: la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP, en adelante), que vuelven a situar al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica y al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, en el centro de la normativa tecnológica de aplicación.

Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de la LRJSP, el ENS insta a los organismos del Sector Público a desarrollar, publicar y hacer valer normas de carácter interno a los propios organismos, tendentes a mejorar el nivel de seguridad de las informaciones que manejan y los servicios que prestan.

DESARROLLO NORMATIVO DE LA POLÍTICA DE SEGURIDAD DEL AYUNTAMIENTO DE GRANADA

Tras la aprobación de la Política de Seguridad de la Información del Ayuntamiento de Granada por la Junta de Gobierno Local el día 31 de marzo de 2017, se hace patente la necesidad de desarrollarla normativamente tal y como aparece explícitamente en muchos de los preceptos del ENS. La Política de Seguridad de la Información del Ayuntamiento de Granada es un documento de alto nivel que define lo que significa 'seguridad de la información' en nuestra organización y se desarrollará, entre otros instrumentos, por medio de la normativa de seguridad, que abordará aspectos generales y específicos y, en general, modelos de comportamiento. La normativa de seguridad estará a disposición de todo el personal del Ayuntamiento de Granada que necesite conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Normativa de Seguridad del Ayuntamiento de Granada trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y desarrollando normativamente la Política de Seguridad del Ayuntamiento de Granada, en segunda instancia.

OBJETIVO DE LA NORMATIVA DE SEGURIDAD "CREACIÓN Y USO DE CONTRASEÑAS EN EL AYUNTAMIENTO DE GRANADA"

El objetivo de la presente normativa de seguridad es regular la creación y uso de contraseñas, cuando éste sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios del Ayuntamiento de Granada.

Contenido

1. OBJETIVO

65. El objetivo de la presente normativa es regular la creación y uso de contraseñas, cuando éste sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios del Ayuntamiento de Granada.

66. Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos siendo la primera línea de protección para las personas usuarias. Una contraseña mal elegida o desprotegida puede resultar en una amenaza de seguridad para toda la

organización. Por ello, todas las personas usuarias de la red corporativa del Ayuntamiento de Granada son responsables de velar por la seguridad de las contraseñas seleccionadas por ellas mismas para el uso de los distintos servicios informáticos municipales.

67. Este documento se considera de uso interno del Ayuntamiento de Granada y por tanto no podrá ser divulgado salvo autorización de la Dirección Técnica del Centro de Proceso de Datos.

2. ÁMBITO DE APLICACIÓN

68. Esta Normativa es de aplicación a todo el ámbito de actuación del Ayuntamiento de Granada y sus Organismos Autónomos, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información del Ayuntamiento de Granada aprobada por la Junta de Gobierno Local el día 31 de marzo de 2017.

69. La presente Normativa será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el Ayuntamiento de Granada, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información del Ayuntamiento de Granada y utilicen contraseñas como medio de autenticación personal.

3. VIGENCIA

70. La presente Normativa ha sido aprobada por la Junta de Gobierno Local del Ayuntamiento de Granada, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que el Ayuntamiento de Granada pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

71. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del Ayuntamiento de Granada.

72. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

4. REVISIÓN Y EVALUACIÓN

73. La gestión de esta Normativa corresponde a la Subdirección de Seguridad de la Dirección Técnica del Centro de Proceso de Datos, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

74. Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), la Subdirección de Seguridad de la Dirección Técnica del Centro de Proceso de Datos revisará la presente Normativa, que se someterá, caso de haber modificaciones, a la conformidad del Comité de Seguridad y aprobación de la Junta de Gobierno Local del Ayuntamiento de Granada.

75. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

76. Será la persona titular de la Subdirección de Seguridad de la Dirección Técnica del Centro de Proceso de Datos la persona encargada de la custodia y divulgación de la versión

aprobada de este documento y será difundido en el Portal del Empleado del Ayuntamiento de Granada.

5. REFERENCIAS

77. Internas:

- Política de Seguridad de la Información del Ayuntamiento de Granada aprobada por Junta de Gobierno Local el día 31 de marzo de 2017
- Documento de Seguridad del Ayuntamiento de Granada

Externas:

- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- Documentos y Guías CCN-STIC.

6. NORMAS PREVIAS

78. La presente “Normativa de creación y uso de contraseñas en el Ayuntamiento de Granada” sustituye, en sus aspectos específicos, a la información contenida en el vigente Documento de Seguridad Municipal que será actualizado en los aspectos señalados en aquella.

7. NORMATIVA

7.1. Uso de contraseñas

79. Las contraseñas (junto con el código de usuario o fichero-id) y/o certificado electrónico son el medio de acceso a sistemas tales como el ordenador del puesto de trabajo, el acceso a la red corporativa, acceso a la cuenta de correo electrónico, acceso a servidores de terminales, acceso al SIM municipal y demás servicios electrónicos. En el control de accesos, el nombre de usuario identifica a la persona usuaria mientras que la contraseña la autentica (con ella se comprueba que es quien dice ser).

80. El Ayuntamiento de Granada dispone de un repositorio de usuarios y contraseñas (Directorio Activo basado en LDAP) y se recomienda que todos los procesos de autenticación para uso de los servicios telemáticos se realicen contra este directorio.

7.2. Cómo crear contraseñas robustas

81. Es necesario que las contraseñas que se utilicen como mecanismo de autenticación sean robustas, es decir, difícilmente vulnerables.

82. Cuestiones previas:

a. Como norma general, las contraseñas deben ser fáciles de recordar y de introducir, aunque difíciles de adivinar y de descubrir por fuerza bruta (prueba exhaustiva de todas las posibilidades).

b. Tradicionalmente, se ha venido sosteniendo que las contraseñas, cuando son elegidas por el usuario, deberían poseer unas ciertas características, entre las que se encontraban: una longitud mínima y la conveniencia de que el conjunto de caracteres escogidos, además de no constituir una palabra de un diccionario, o una fecha, o un nombre propio, debería ser una combinación de letras mayúsculas y minúsculas, números y signos de puntuación.

c. Sin embargo, la dificultad de recordar contraseñas construidas de la forma anterior (lo que suele provocar que los usuarios opten por escribir tales contraseñas en papel o en lugares no protegidos), junto con el incremento de la potencia de los ordenadores, han hecho que este procedimiento de generación de contraseñas no sea tan eficaz como originariamente pudo parecer. Por el contrario, la complejidad en la elección de una contraseña se determina usando el concepto de entropía, derivado de la Teoría de la Información de Shannon.

83. En este sentido, se han definido los siguientes aspectos y reglas, que deberán ser observados por todo el personal a la hora de la definición o creación de contraseñas robustas:

a. La longitud de la contraseña debe ser como mínimo de 8 caracteres, si bien se recomienda usar contraseñas más largas. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.

b. Se utilizará la concatenación de varias palabras para construir contraseñas largas (passphrases) cuya deducción, automática o no, no sea simple. Por ejemplo: “elefanteneumáticocarpeta”, incluso contemplando la presencia de espacios en blanco. Por ejemplo: “cocina televisor ventana”. También pueden utilizarse frases cortas sin sentido.

c. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”) así como no repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

d. Las contraseñas no deberán estar compuestas de datos propios que otra persona pueda adivinar u obtener fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, etc.), ni ser frases famosas o refranes, ni ser estrofas de canciones o frases impactantes de películas o de obras de literatura.

e. Las contraseñas deberán ser fáciles de recordar. Se hace necesario, por tanto, encontrar una solución de compromiso entre la robustez de la contraseña y la facilidad con la que se puede recordar.

f. Hay que evitar apuntar las contraseñas en papel ni guardarlas en un archivo sin cifrar o bajo otro procedimiento o contenedor no seguro.

g. La contraseña no deberá ser igual a ninguna de las últimas contraseñas usadas, ni estar formada por una concatenación de ellas.

h. La contraseña deberá cambiarse como mínimo una vez al año en todos los sistemas y servicios informáticos que permitan que el usuario modifique autónomamente su contraseña o bien siempre que se entienda que la contraseña haya podido ser puesta en compromiso.

i. Cuanto más sensible, confidencial o protegida sea la información con la que se trabaja, más recomendable es el robustecimiento de las contraseñas y el aumento de la frecuencia de cambio de las mismas.

j. Es especialmente importante mantener el carácter secreto de la contraseña. No debe entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata.

k. No utilizar la misma contraseña para distintos servicios web externos o en el acceso a distintos dispositivos.

7.3. Cambio de contraseña

84. Si un usuario entiende que su contraseña ha quedado comprometida o la ha cedido a terceros autorizados por motivos de trabajo o mantenimiento, debe proceder a sustituirla por otra que no hubiere sido comprometida, de manera inmediata.

85. Por otro lado, cuando se produzca alguna de las situaciones siguientes:

a. Olvido de la contraseña.

b. Bloqueo del acceso a través de contraseña tras cinco intentos fallidos.

La persona usuaria o bien usará las utilidades al efecto existentes en el Portal del Empleado o realizará una petición de cambio de contraseña a la Dirección Técnica del Centro de Proceso de Datos, a través del Centro de Atención de Usuarios (C.A.U.).

86. En estos casos, como norma general, el cambio de contraseña por una contraseña provisional (generalmente, de un solo uso) será realizado por personal técnico de Dirección Técnica del Centro de Proceso de Datos, que, por los medios que se establezcan, comunicará esta contraseña al usuario, sin intermediarios.

87. Las contraseñas proporcionadas por la Dirección Técnica del Centro de Proceso de Datos, tras la petición de cambio de contraseña de un equipo y/o aplicaciones, son consideradas contraseñas “provisionales” y son muy inseguras. Por ello, el usuario deberá proceder a sustituir la contraseña “provisional” por una contraseña personal que cumpla con los requisitos indicados en el apartado anterior. El usuario deberá realizar este cambio durante el primer inicio de sesión en su puesto de usuario.

88. Ningún usuario está autorizado a acceder a los servicios internos del Ayuntamiento de Granada utilizando la identidad (usuario+contraseña o certificado electrónico) de otros usuarios, incluyendo el simple conocimiento de la contraseña de otro usuario. Esta práctica compromete la confidencialidad de la información, y por supuesto, la autenticidad de quién accede a ella.

7.4. Gestión de contraseñas

89. El Ayuntamiento de Granada, a través de la Dirección Técnica del Centro de Proceso de Datos, decidirá sobre la oportunidad de que ciertos usuarios puedan utilizar programas gestores de contraseñas.

90. Desde la Dirección Técnica del Centro de Proceso de Datos, deben detectarse los intentos repetidos y erróneos de identificación y tratarlos como posibles ataques de descubrimiento por el método de prueba-error. Se establece un retardo de quince minutos para el desbloqueo automático de una cuenta bloqueada y cinco intentos erróneos de identificación para la suspensión temporal y cautelar de la cuenta.

7.5. Contraseñas de servicios y servidores

91. Las siguientes reglas de uso van dirigidas al personal municipal que administre o sea responsable de algún servidor o servicio tecnológico que sea accesible a distintos usuarios (externos o internos):

a. Los servidores y dispositivos se deben configurar con cuentas separadas para los que tienen privilegios de administración y los que no.

b. Las personas usuarias se deberían autenticar con cuentas que no tuvieran más privilegios que los necesarios para hacer uso del servicio. A tal efecto, al personal municipal que administre o sea responsable de algún servidor o servicio tecnológico podrán tener más de una cuenta identificativa para cada rol privilegiado.

c. Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deberán tener contraseñas distintas a otras cuentas mantenidas por dicho usuario en los servicios y recursos.

d. Se evitará el uso de autenticación con usuarios genéricos como Administrador, debiendo utilizar cuentas personales de usuario privilegiadas con los roles correspondientes.

e. Si es posible, el acceso a los privilegios correspondientes (para administrar la máquina) debe hacerse mediante mecanismos de “escalado de privilegios”; en este caso además quedará traza de qué usuario ha accedido a estos privilegios especiales.

f. Sólo se tendrán los privilegios especiales el tiempo que sea estrictamente necesario.

g. Se deberá dar de baja inmediatamente las cuentas privilegiadas de aquellos usuarios que dejen de administrar el servicio tecnológico.

h. Es necesario cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

i. Para el acceso a la administración de sistemas y servidores se observarán todos los requisitos del apartado “Cómo crear contraseñas robustas” con la única salvedad de que las contraseñas deberán tener una longitud igual o superior a 10 caracteres.

92. Desde la Dirección Técnica del Centro de Proceso de Datos, se ejecutará al menos una vez al año, una aplicación de descubrimiento de contraseñas de los usuarios, especialmente de aquellos que administren o sean responsables de algún servidor o servicio tecnológico. Para las contraseñas que no superen el programa de descifrado de contraseñas se aplicará un mecanismo en dos fases: en las primeras 24h, si el usuario accede al sistema, se le obligará a modificar su contraseña. Pasadas las 24h, la contraseña se anula y el usuario habrá de pasar por un proceso completo de autenticación

7.6.- Desarrollo de aplicaciones y contraseñas

93. Los desarrolladores de aplicaciones informáticas para el entorno del Ayuntamiento de Granada y que gestionen sus propios mecanismos de autentificación mediante contraseñas, deben asegurarse de que sus programas contienen las siguientes precauciones en términos de seguridad respecto de la selección y uso de contraseñas:

a. Deben soportar autenticación de usuarios individuales, no por grupos.

b. No deben almacenar contraseñas en texto claro o en ninguna forma fácilmente reversible.

c. Deben proveer de algún tipo de mecanismo de roles, de forma que un usuario pueda tomar las funciones de otro sin necesidad de conocer la contraseña del anterior.

d. Deben proveer de un mecanismo para expirar las contraseñas y obligar a los usuarios al cambio de la misma.

e. Se debe limitar el número de intentos de accesos sin éxito consecutivos.

8.- RESPONSABILIDADES

94. El incumplimiento de la presente Normativa puede llegar a comprometer la seguridad de la totalidad de la red corporativa del Ayuntamiento de Granada.

95. Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, la Dirección Técnica del Centro de Proceso de Datos podrá proceder al bloqueo temporal o indefinido del usuario dependiendo de la gravedad y reiteración del incidente, siendo responsable el usuario titular. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.”

Por todo lo expuesto y a propuesta del Teniente de Alcalde Delegado de Economía, Hacienda, Personal, Contratación, Organización y Smart City, la Junta de Gobierno Local, por unanimidad de los presentes, **acuerda:** Aprobar la Normativa de Seguidad: “Creación y uso de contraseñas en el Ayuntamiento de Granada” de conformidad con el texto arriba transcrito.”