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:

CENTRO DE PROCESO DE DATOS

569

Aprobación de la normativa de seguridad: Almacenamiento de información en sistemas informáticos del Ayuntamiento de Granada.

Visto expediente **núm. 153/2018** del Centro de Proceso de Datos, relativo a la **Aprobación de la normativa de seguridad: Almacenamiento de información en sistemas informáticos del 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: "Almacenamiento de Información en Sistemas Informáticos del Ayuntamiento de Granada", del siguiente tenor literal:

"INTRODUCCIÓN

La creciente dependencia de la mayoría de las organizaciones de sus sistemas de información pone de manifiesto la necesidad de contar con medios y técnicas que permitan almacenar la información de la manera más eficiente y adecuada, preservando la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de los activos de información.

El establecimiento de procedimientos, planes y políticas de almacenamiento, conservación, recuperación y borrado es esencial para garantizar la seguridad de un activo tan importante para una organización como es la información.

Por otra parte, siendo el almacenamiento un recurso limitado, el crecimiento exponencial de los datos hace que las organizaciones se enfrenten a la necesidad de regular y simplificar la gestión de la información, mejorando la eficiencia del almacenamiento y su protección mediante instrucciones a las personas usuarias y mediante tecnologías como instantáneas, encriptación, replicación e integración, compactación de datos, etc.

En particular, en el Ayuntamiento de Granada, los Sistemas de Información y el tratamiento de la información constituyen elementos básicos para el desarrollo de sus actividades y servicios a la ciudadanía, por lo que las personas usuarias deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados.

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 todos los miembros del Ayuntamiento de Granada que necesiten 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 "ALMACENAMIENTO DE INFORMACIÓN EN SISTEMAS INFORMÁTICOS DEL AYUNTAMIENTO DE GRANADA"

El objetivo de la presente normativa de seguridad es regular y asegurar la operación eficiente y segura del almacenamiento de información en los sistemas informáticos del Ayuntamiento de Granada.

Contenido

1. OBJETIVO

1. El objetivo de la presente normativa de seguridad es regular y asegurar la operación eficiente y segura del almacenamiento de información en los sistemas informáticos del Ayuntamiento de Granada.

2. Los Sistemas de Información y el tratamiento de la información constituyen elementos básicos para el desarrollo de las actividades del Ayuntamiento de Granada y sus servicios a la ciudadanía, por lo que el personal municipal debe utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

3. 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

4. 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 Junta de Gobierno Local el día 31 de marzo de 2017.

5. 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.

3. VIGENCIA

6. 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.

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

8. 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

9. 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.

10. 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.

11. 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.

12. 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

13. 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

14. La presente "Almacenamiento de Información en Sistemas Informáticos del 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. Gestión del almacenamiento de la información municipal

15. Es función de la Dirección Técnica del Centro de Proceso de Datos el aprovechamiento, gestión y optimización de los recursos informáticos disponibles en al Ayuntamiento de Granada, incluso de aquellos que sean aportados por otras áreas o servicios.

16. Para la planificación de los recursos disponibles se requiere la colaboración y coordinación de todos los departamentos, servicios, áreas y concejalías, que comunicarán cualquier plan que pueda afectar o requiera el uso de los recursos informáticos municipales. La Dirección Técnica del Centro de Proceso de Datos establecerá tantas medidas como sean necesarias y posibles para ofrecer un servicio adecuado.

17. Para aquella información y contenidos alojados en los sistemas de almacenamiento de ordenadores y servidores propiedad de la Administración Municipal, la Dirección Técnica del Centro de Proceso de Datos realizará la atribución concreta de espacio de memoria según los recursos disponibles.

18. La Dirección Técnica del Centro de Proceso de Datos puede limitar o controlar los servicios de almacenamiento por motivos de seguridad o rendimiento de la Red Informática Municipal de Granada. Se podrán establecer aquellas limitaciones técnicas que la Dirección Técnica del Centro de Proceso de Datos considere oportunas para un mejor desarrollo del servicio.

7.2 . Derechos, obligaciones y límites en el almacenamiento de la información municipal

19. El personal del Ayuntamiento de Granada que requiera la utilización de cualquier servicio de almacenamiento adicional al asignado inicialmente, deberá solicitar autorización a sus responsables directos, ya que son éstos los que conocen el alcance de las labores a

desarrollar, y por tanto las herramientas que le son necesarias. Así mismo, el responsable podrá solicitar asesoramiento de la Dirección Técnica del Centro de Proceso de Datos para la elección entre las mejores herramientas disponibles.

20. El personal municipal, en base a la autorización de acceso al Sistema de Información Municipal, obtendrá un identificador que le faculta inicialmente el acceso al almacenamiento local del equipo informático asignado, a la carpeta Unidad y a la carpeta de red denominada con el identificador correspondiente. Además podrá acceder a las unidades de red restringidas del Área o Servicio para las que tenga autorización.

21. En los sistemas informáticos municipales, no se podrá almacenar información ilegal, abusiva, difamatoria, racista, ofensiva, o cualquier otro tipo de información susceptible de objeción, ya sea mediante fotografías, textos, banners publicitarios, etc. Tampoco se podrán infringir derechos de propiedad intelectual o cualquier otra información que el Ayuntamiento de Granada considere inapropiada siendo responsable directo el infractor y debiendo responder ante el Organismo competente.

22. Cualquier uso del servicio de almacenamiento para fines ilícitos autorizará a la Dirección Técnica del Centro de Proceso de Datos del Ayuntamiento de Granada a suspender el acceso al mismo por parte de la persona responsable sin previo aviso.

23. El Ayuntamiento de Granada se reserva el derecho a denegar o cancelar el servicio si se incurre en cualquier conducta o actividad que se considere abuso o violación de alguno de los términos, normas y condiciones aquí expuestas:

a) La utilización del servicio de almacenamiento del Ayuntamiento de Granada se ajustará a lo dispuesto en la legislación vigente, especialmente en materia de protección de datos de carácter personal, propiedad intelectual e industrial y protección del honor e intimidad y, en su caso, a las normas propias de este Ayuntamiento que resulten aplicables.

b) Como práctica general, se prohíbe realizar cualquier acto que interfiera en el correcto funcionamiento de los recursos de almacenamiento municipales.

c) No está permitido realizar acciones que deterioren o incrementen en exceso la carga de los recursos informáticos, hasta el límite de llegar a perjudicar a otros usuarios o al rendimiento de los mismos.

d) Se prohíbe cualquier actividad que suponga violar la privacidad de los datos y el trabajo de los otros usuarios. En particular, se prohíbe el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiere sido previamente autorizada.

e) Toda información que se encuentre protegida por derechos de autor que sea titularidad de terceros o del Ayuntamiento de Granada deberá utilizarse con arreglo a la legislación vigente y a la normativa municipal.

24. Además, todas las personas que accedan a los servicios de almacenamiento corporativos están obligados a:

a) Hacer un uso diligente del espacio de almacenamiento, guardando sólo aquella información necesaria.

b) A respetar las cuotas de almacenamiento asignado, si las hubiere.

c) Eliminar carpetas y ficheros obsoletos o que no se van a usar

d) En el caso de usar programa cliente de sincronización, cumplir con las medidas de seguridad estipuladas con el fin de impedir accesos no autorizados a la información personal o de grupo.

e) En el caso de usar programa cliente de sincronización, ser cauteloso con la actividad en la carpeta local para impedir borrados accidentales masivos o indeseados.

f) Evitar el almacenamiento de ficheros especialmente grandes, si no es estrictamente necesario su uso, en las unidades de almacenamiento de red.

7.3. Almacenamiento local

25. El personal municipal utiliza equipos informáticos para realizar su actividad profesional. La información se genera en estos equipos y desde ellos se modifica y transmite. Cada uno de estos equipos dispone de un sistema de almacenamiento local, normalmente discos duros (unidad C o unidad D) donde se guarda la información.

26. Con carácter general, la información almacenada de forma local en los equipos informáticos no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, no se recomienda a los usuarios el almacenamiento local de la información importante para el desarrollo de su actividad profesional.

27. La información institucional que se almacene en los equipos informáticos debe ser trasladada diariamente a los Servidores de almacenamiento en red.

7.4. Almacenamiento en red

28. Para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir información entre las diferentes grupos, áreas y personas empleadas municipales, el Ayuntamiento de Granada dispone de servidores de almacenamiento en red (habitualmente unidades F,G, H, P, ..).

29. La Dirección Técnica del Centro de Proceso de Datos se encargará de proveer el espacio de almacenamiento necesario en función de los recursos disponibles. Para un mejor reparto del espacio de disco y demás recursos podrán establecerse cuotas de disco. Así mismo dedicará los recursos adecuados, más seguros, rápidos y fiables que sea posible, debido a la importancia de estas carpetas.

30. Las personas usuarias tendrán autorizado el acceso únicamente a aquella información y recursos de almacenamiento de red que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

31. No está permitido almacenar información privada, de cualquier naturaleza, ni archivos de vídeo, música y fotos que no sean de carácter institucional en los recursos de almacenamiento en red o compartidos, salvo autorización previa de la Dirección Técnica del Centro de Proceso de Datos.

32. Debido a las características técnicas de los elementos físicos (hardware) y lógicos (software) dedicados al servicio de almacenamiento en red, el coste de mantenimiento es muy alto, por lo que no podrán ser usadas para otras funciones que no sean las ya indicadas.

7.4.1. Uso de las unidades de red.

33. Las unidades de red (unidades F, G, H,…P,Q..) se utilizarán para los archivos que sean necesarios de forma habitual para el trabajo diario.

34. A las carpetas ubicadas en la unidad G: se les denomina “carpetas departamentales”. La tendencia será la de una carpeta por departamento, área o Concejalía, en función del tamaño y del uso requerido.

35. Se deberá evitar el tratamiento en las unidades de red de toda la información de datos de carácter personal, o de naturaleza técnica o institucional, que sea inadecuada, excesiva, innecesaria o desfasada.

36. La información almacenada en las unidades de red y carpetas departamentales contará con los esquemas de respaldo y seguridad necesarios para garantizar su disponibilidad, confidencialidad e integridad

37. Las unidades de red nunca deben dedicarse o usarse como:

a) Copia de seguridad de los datos del disco duro propio.

b) Copia de seguridad del correo electrónico.

c) Copia de seguridad de las propias carpetas departamentales o de las de otros departamentos.

d) Alojamiento de software para instalar salvo autorización previa de la Dirección Técnica del Centro de Proceso de Datos.

e) Alojamiento de archivos bajados de Internet, a no ser que sean necesarios para el trabajo.

f) Alojamiento de grandes archivos (superiores a 1GB) salvo autorización previa de la Dirección Técnica del Centro de Proceso de Datos quién determinará los formatos de almacenamiento permitidos.

38. Caso de ser necesario hacer referencia a un mismo documento o información en una carpeta distinta a la de su carpeta de origen, en lugar de copiar se realizará referencia mediante accesos directos, evitando la duplicidad de dicha información.

7.4.2. Uso de la carpeta de intercambio Unidad

39. La finalidad de la carpeta G:\Unidad es la de intercambiar o depositar temporalmente información cuando ésta no pueda transmitirse por otros medios de la Intranet municipal, como la aplicación de intercambio de ficheros o los ficheros anexos a mensajes de correo electrónico. Caso de ser necesario el intercambio de archivos, se utilizará exclusivamente las carpetas denominadas Unidad o bien aplicaciones establecidas corporativamente a tal efecto.

40. La información deberá permanecer en G:\Unidad el menor tiempo posible, por lo que el usuario depositante procederá a extraerla e incorporarla o a un dispositivo o a una ubicación seguros de acceso restringido, o a suprimirla lo antes posible.

41. La Dirección Técnica del Centro de Proceso de Datos podrá eliminar periódicamente la información contenida en G:\Unidad

7.4.3. Auditoría, seguridad y permisos.

42. Todos los archivos y carpetas alojados en los servidores municipales dispondrán de permisos de acceso según las indicaciones del/la Coordinador/a, Directora/a General, Jefe/a de Servicio, Jefe de la Policía Local o SPEIS o personas designadas por estos últimos (responsable de la carpeta) en carpetas del Área de su competencia.

43. Los permisos se otorgarán a grupos de usuarios y podrán ser: sólo lectura o lectura-escritura-borrado. La asignación de permisos, solo se llevará a cabo hasta un tercer nivel en las ramas del árbol principal de las carpetas pertenecientes a un Área. Las modificaciones de los permisos serán por petición del/la Coordinador/a, Directora/a General, Jefe/a de Servicio, Jefe de la Policía Local o SPEIS o personas designadas por estos últimos (responsable de la carpeta) y por el cauce habitual.

44. Periódicamente o a petición de los responsables de carpetas podrán realizarse auditorías de acceso, borrado, lectura, acceso denegado, etc. Dicha auditorías serán entregadas al responsable de la carpeta para su estudio, no siendo función de la Dirección

Técnica del Centro de Proceso de Datos aspectos no técnicos de las mismas, si bien asesorará tanto como sea necesario desde el punto de vista tecnológico.

45. Las auditorías de carpetas que realice de oficio la Dirección Técnica del Centro de Proceso de Datos sólo podrán tener como objeto la detección de averías, la prevención de falta de espacio, el aviso a usuarios de errores cometidos de forma involuntaria, eliminación de archivos expresamente prohibidos, estadística para mejoras futuras y cualquier otro aspecto que mejore el sistema.

7.4.4. Copia de seguridad del almacenamiento de red

46. Se realizarán copias de seguridad de los datos que residan en los servidores de almacenamiento en red municipales en los tiempos establecidos por la legislación vigente, llevadas a cabo por la Dirección Técnica del Centro de Proceso de Datos, con el fin de ofrecer un servicio de recuperación de ficheros perdidos, borrados o deteriorados

47. Toda información o dato que por cualquier motivo tenga obligación de mantener una copia de seguridad será alojado en una carpeta departamental autorizada del servidor que corresponda.

48. Los encargados de las aplicaciones, especialmente las afectadas por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por el Reglamento General de Protección de Datos (RGPD) , deberán indicar las necesidades de copia de seguridad específicas.

49. Existe un procedimiento para sistematizar la realización de copias de respaldo de toda la información generada en el Ayuntamiento, en soportes externos (habitualmente en cintas.) y almacenados en otra ubicación distinta al Centro de Proceso de Datos para recuperación en caso de desastre.

50. Las copias de seguridad de los sistemas de almacenamiento podrán ser aumentadas en frecuencia si un departamento así lo solicitase y justificase, especialmente para el mejor cumplimiento de reglamentos, leyes o normas de seguridad.

51. La tendencia de la Dirección Técnica del Centro de Proceso de Datos será la copia de seguridad diaria.

52. El personal empleado municipal podrá solicitar la restauración de un fichero borrado accidentalmente o dañado indicando el nombre del fichero a recuperar y la localización exacta del mismo, teniendo en cuenta que el fichero se recuperará sobre la misma unidad de red.

7.5. Almacenamiento en dispositivos externos

53. Dispositivos externos. Adicionalmente se puede disponer de sistemas externos que, conectados directamente a los equipos, permiten un almacenamiento extra de la información, evitando que se ocupe este espacio en el equipo. Estos pueden ser cintas magnéticas, discos duros externos, CD o DVD o pendrives conectados a través de distintos interfaces físicos. Existen también dispositivos externos que se pueden conectar de forma inalámbrica. Los distintos tipos de interfaz tienen también distinta velocidad de transferencia. Por su portabilidad es fácil que se puedan extraviar así que deben ser previamente autorizados.

54. 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 dispositivos externos de almacenamiento masivo de la información (pendrive, grabadoras de CD o DVD, etc). 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.

7.6. Almacenamiento en la nube

55. La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio (CSP, Cloud Service Provider). Ofrece grandes beneficios como pueden ser la deslocalización, la alta disponibilidad, el acceso a información desde cualquier lugar, la flexibilidad en asignación de recursos y un ahorro económico significativo.

56. El almacenamiento en la nube es una manera sencilla y escalable de almacenar, acceder y compartir datos a través de Internet. Los proveedores de almacenamiento en la nube son propietarios y responsables del mantenimiento del hardware y software conectados en red, mientras que las personas usuarias se dedican a aprovisionar y utilizar lo que necesiten por medio de una aplicación web o propietaria.

57. Con carácter general no se permite el uso de servicios en nubes públicas, salvo autorización de la Dirección Técnica del Centro de Proceso de Datos.

58. Al usar servicios en la nube, el Ayuntamiento de Granada debe seguir los mismos criterios de seguridad usados para la información asociada a los servicios contratados, reflejándolo en los Acuerdos de Nivel de Servicio que se firmen con el proveedor (CSP) y además tanto Ayuntamiento como CSP deben tener en cuenta aquellos criterios de seguridad enumerados en la Guía de Seguridad (CCN-STIC-823) “Utilización De Servicios en la Nube”, en particular los relativos a gestión de riesgos, gestión de servicios externos y a efectos de disponibilidad, el CSP deberá cumplir todas las medidas del Anexo II del ENS pertinentes para el nivel de disponibilidad requerido y aquellas de nivel medio a efectos de Integridad, Confidencialidad, Autenticidad y Trazabilidad aplicación y otros requisitos legales como los provenientes de la RGPD y LOPD.

59. Toda la información y datos del Ayuntamiento de Granada que vayan a ser almacenados en la nube, deberán ser cifrados antes de su salida y se comunicarán cifrados, de forma que el Ayuntamiento será el único en poder de las claves de cifra, a las que aplicará lo previsto en el Anexo II del ENS.

60. El proveedor CSP deberá disponer de un procedimiento de copias de seguridad que garantice la restauración de la información. El proveedor CSP deberá informar al Ayuntamiento de Granada de aspectos relativos a alcance de los respaldos, Política de copias de seguridad, medidas de cifrado de información en respaldo y procedimiento de solicitud de restauraciones.

61. El proveedor CSP a la finalización de la relación contractual, en el plazo más breve posible, estará obligado a entregar toda la información al Ayuntamiento de Granada garantizando la integridad de la misma. Posteriormente, el proveedor CSP eliminará la información, tras la finalización de las obligaciones de retención de datos que pudieran ser obligatorias por política o por imperativo legal, debiendo garantizar la efectiva destrucción de toda la información.

7.8. Eliminación segura de los medios de almacenamiento

62. La Dirección Técnica del Centro de Proceso de Datos debe garantizar los mecanismos necesarios para eliminar de manera segura la información contenida en los puestos de escritorio, portátiles y demás recursos informáticos, cuando éstos cambian de usuario o son dados de baja. Así mismo, debe definir procedimientos para la destrucción y/o eliminación segura de los medios de almacenamiento de la información acorde con la Políticas vigentes.

8.- RESPONSABILIDADES

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

64. 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 Seguridad: “Almacenamiento de información en sistemas informáticos del Ayuntamiento de Granada” de conformidad con el texto arriba insertado.”