NORMATIVA

USO DE DISPOSITIVOS DE MEMORIA EXTRAIBLES

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.23	DOCUMENTO:	NORMATIVA DE USO DE DISPOSITIVOS DE MEMORIA EXTRAÍBLES

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	31 – Octubre - 2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
[ÁREA]	[ÁREA]	Comité de Seguridad de la Información
[NOMBRE – INICIALES]	[NOMBRE – INICIALES]	[NOMBRE – INICIALES]
FECHA:	FECHA:	FECHA:
FIRMA:	FIRMA:	FIRMA:

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	☐	PUBLICABLE	☐	USO INTERNO	☒	CONFIDENCIAL:	☐	SECRETA:	☐

PRIVACIDAD

NO IP	☐	IP A	☒	IP B	☐	IP C	☐

Confidencialidad Acerca de este documento

Excmo. Ayuntamiento de Baeza

Pje. Cardenal Benavides, 10
23440 Baeza, Jaén
ESPAÑA
http://www.baeza.es/baeza/extranet/

1) OBJETO

Esta normativa tiene por objeto establecer las reglas de uso de los medios de almacenamiento extraíbles, tales como memorias USB o discos portátiles utilizados en el Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

2) ALCANCE

Es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, presta sus servicios al Ayuntamiento, incluyendo proveedores externos cuando sean usuarios de los Sistemas de Información la entidad.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de la Entidad, Responsable de Seguridad, Responsable del Sistema y de todos los actores intervinientes en la misma.

Cualquier modificación posterior entrará en vigor al día siguiente de su aprobación y publicación por parte del Comité de Seguridad. En este caso, la versión anterior quedará anulada por la última versión de esta normativa.

3) RESPONSABILIDADES

La responsabilidad de poner en marcha las medidas descritas en la presente normativa recae sobre el Responsable del Sistema, que ejecutará a través del departamento de sistemas. Podrá delegar dicha responsabilidad en el Administrador de Seguridad.

4) DESARROLLO NORMATIVO

4.1) COPIA Y TRANSPORTE DE INFORMACIÓN

A. Solo podrán existir medios removibles con información confidencial o de carácter personal por necesidades de trabajo del Ayuntamiento.
B. Se podrá copiar y transportar información en soportes extraíbles, siempre que se cumplan los requisitos siguientes:
    1. Disponer de autorización expresa por parte del Administrador de Seguridad.
    2. Las memorias extraíbles serán las proporcionadas por el Ayuntamiento, siendo de uso exclusivo para el puesto autorizado, no debiendo ser usado en puestos ajenos.
    3. Para información PÚBLICA: Se podrá almacenar información pública sin necesidad de cifrar.
    4. Para información de USO INTERNO: Podrá almacenar la información de Uso Interno, cifrado o sin cifrar, todo el personal del Ayuntamiento y personal externo que esté autorizado por el Responsable de Seguridad o esté directamente relacionado con el desempeño de sus funciones dentro de la entidad.
    5. Para información CONFIDENCIAL: sólo el personal del Ayuntamiento autorizado a acceder y a tratar la información podrá almacenarlos en memorias extraíbles. Cuando el soporte vaya a salir fuera de las instalaciones del Ayuntamiento se cifrará necesariamente. Dentro de las instalaciones no será necesario
    6. Para información SECRETA: se podrá almacenar información solamente por el personal del Ayuntamiento que esté expresamente autorizado a acceder y tratar la información. Será necesario el cifrado de la información en el soporte, tanto si este va a salir de las dependencias del Ayuntamiento como si no.
C. Cuando los dispositivos extraíbles estén fuera de las instalaciones del Ayuntamiento o en lugares de acceso libre, no se abandonarán en ningún momento, o se guardarán en lugares de acceso restringido, como por ejemplo cualquier sitio que necesite llave para acceder.
D. En caso de no ser posible la realización de este formateo lógico por parte de un usuario, este medio será llevado al Administrador de Seguridad para proceder a su borrado lógico seguro con la mayor diligencia posible.

E. En caso de tratarse de un disco duro que haya formado parte de servidor, se formateará de manera segura igual que cualquier otro disco que pueda contener información sensible o confidencial.
F. Las devoluciones o bajas de ordenadores de sobremesa o portátil realizadas al Administrador de Seguridad se tratarán igual que otro medio lógico formateable. Una vez realizado este borrado y comprobado su estado, se cerrará la asignación al usuario sobre ese equipo, y adicionalmente se modificará el registro del equipo en el inventario para cambiar su estado de Uso a Almacén, en caso de que el equipo sea reutilizable, o a Baja, en caso de que el equipo no sea reutilizable. Si el equipo ya no es reutilizable y su estado cambia a Baja, se etiquetará como Baja y se reusarán los componentes en caso de que sean utilizables para futuras reparaciones.
G. El almacenamiento de los dispositivos se realizará respetando las recomendaciones del fabricante.
H. El almacenamiento de los medios removibles se realizará siempre siguiendo las directrices dictadas en la política que se creará con el nombre de: “Política de escritorio y pantalla limpios”.
I. El etiquetado, almacenado y gestión de las cintas de Backup se realizará siguiendo las directrices dictadas en: “Política de Copias de seguridad, restauración y verificación”.

J. En todo caso, el usuario del dispositivo de memoria es el custodio de la información contenida en el mismo, así como el responsable directo del uso que se hace de el.

4.2) DESTRUCCIÓN DE MEDIOS REMOVIBLES

A. Se destruirá el medio removible cuando este ya no sea necesario o haya alcanzado su fin de vida.
B. Para realizar una destrucción segura de dispositivos removibles se tratarán todos los medios como si contuviesen información confidencial. El propósito de esta medida es evitar el etiquetado de los medios sensibles, el cual supone un riesgo al marcar dispositivos haciéndolos más llamativos.
C. La destrucción de papeles se realizará en las destructoras de papel si pudiera contener información confidencial inmediatamente después de haber terminado la tarea por su uso.
D. La destrucción de medios se realizará en el momento de la recepción del dispositivo. No se permite acumular dispositivos con información confidencial o sensible para no aumentar la cantidad de la misma con posibilidad de recuperación.
E. Si la destrucción lógica de la información de un medio lógico no fuera posible (CD/DVD/HD defectuoso/USB), se realizará la destrucción del medio a través de un método físico que impida la reconstrucción total o parcial del medio.
F. Los medios de Backup serán borrados tras su fin de vida. Se borrarán usando una técnica de borrado seguro con sobreescritura de datos. Posteriormente se retirará la etiqueta descriptiva del medio de Backup para su destrucción.
G. Cuando el Responsable del Sistema realice una eliminación física de un medio confidencial se creará un registro de seguridad en el sistema de gestión de incidencias.

5) RESPONSABLE DEL PROCEDIMIENTO

El Responsable de Seguridad, velará por el cumplimiento de la presente Norma, informando al Comité de Seguridad de la Información sobre los incumplimientos o deficiencias de seguridad observados para que se tomen las medidas oportunas.

6) REFERENCIAS

- 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 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.
- Guía de Seguridad CCN-STIC 821: Normas de Seguridad.
- Guía de Seguridad de las TIC CCN-STIC 883: Guía de Implantación del ENS para Entidades Locales.
- Guía de Seguridad CCN-STIC 804: Guía de Implantación.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- RGPD (UE) 2016/679, del parlamento europeo y del consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos..
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.
- Política de escritorio y pantalla limpios.
- Normativa de Backups, restauración y verificación.

7) REGISTROS/ANEXOS