NORMATIVA

BACKUPS, RESTAURACIÓN Y VERIFICACIÓN

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.10	DOCUMENTO:	NORMATIVA DE BACKUPS, RESTAURACIÓN Y VERIFICACIÓN

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/

BACKUPS, RESTAURACIÓN Y VERIFICACIÓN

Elaborado por: Fecha:	Revisado por: Fecha:	Aprobado por: Fecha:

MODIFICACIONES DESDE LA ÚLTIMA EDICIÓN
-

A) OBJETO

El objeto de esta normativa es el de determinar el mecanismo para la planificación, revisión, almacenamiento, herramientas y pruebas de restauración que pondrá en marcha el Excmo. Ayuntamiento de Baeza. (en adelante Ayuntamiento) para la realización de copias de seguridad. Igualmente se definirá el procedimiento de realización y restauración de esas copias de seguridad.

B) ALCANCE

Esta normativa afecta a todo el personal del Ayuntamiento y a todos los sistemas de la información de 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.

C) RESPONSABILIDADES

La responsabilidad del control, verificación y realización de copias de seguridad recae sobre el Administrador de Seguridad, el cual podrá delegar dicha tarea o alguna de ellas a la persona o personas que posean los conocimientos necesarios para el desempeño de las funciones encomendadas.

D) DESARROLLO DE LA NORMATIVA

El mantenimiento de la seguridad e integridad de los datos almacenados en los servidores del Ayuntamiento requiere de métodos que aseguren que dichos datos son salvaguardados mediante una serie de normas, procedimientos y niveles de seguridad. Estas normas, procedimientos y niveles deben asegurar todo el ciclo de vida de una copia de seguridad, incluyendo su manipulación física, para garantizar un correcto almacenamiento y acceso a la información almacenada para su restauración en caso de ser necesaria.

D.1) COPIAS DE SEGURIDAD

Dependiendo de la arquitectura de cada sistema de información del Ayuntamiento y las funciones que desempeñe, deben adaptarse los procedimientos empleados: "*Procedimiento de Copias de Seguridad (backup)*" y "*Procedimiento de Restaurado de Información*" para llevar a cabo las copias de respaldo.

D.2) PLANIFICACIÓN

Atendiendo a la importancia de la información contenida en cada sistema, a su criticidad y a las características de aquéllos, se elaborará una planificación de copias de seguridad donde deben incluirse todos los sistemas existentes en el momento y permitir una fácil escalabilidad para contemplar la incorporación de sistemas futuros.

Las copias de seguridad se realizarán una vez al día, excepto cuando se sepa que, para algún sistema, la información no cambia.

Las copias de seguridad serán planificadas para ser ejecutadas en horas en las que interfiera lo menos posible con los servicios ofrecidos. Siempre que sea viable, la copia se realizará sin detener el servicio.

Para aquellos sistemas que, por sus peculiaridades, no puedan ser incorporados en la planificación de copias de seguridad común establecida, deben disponer de un sistema de copias de seguridad alternativo que garantice su recuperación.

Adicionalmente a la información en sí, se deberá guardar copia de seguridad de todo aquel software activo en los sistemas, para su restauración completa en caso de desastre.

D.3) REVISIONES

Se revisará, de acuerdo con la frecuencia de ejecución y lo antes posible tras su finalización, los registros de las copias de seguridad realizadas e intentos fallidos. Aquellas que hayan fallado deben ser planificadas para ser ejecutadas cuanto antes, sin que interfieran con el resto de la planificación definida de copias a ejecutar.

Se mantendrá un historial de incidencias de copias de seguridad y será revisado periódicamente de modo que se facilite la identificación de errores ya existentes y se optimice el tiempo de resolución de los mismos.

Deberán tomarse las medidas necesarias para mantener actualizada la planificación de copias de seguridad, de modo que se contemple la inclusión de nuevos tratamientos o modificaciones en los sistemas relacionados.

D.4) ALMACENAMIENTO

Las copias de seguridad realizadas se almacenarán en un recinto ignífugo y resistente a agentes corrosivos externos.

También se podrán almacenar copias de seguridad, de carácter digital, en servicios de almacenamiento en la nube, siempre y cuando, cumplan con los requisitos exigidos por la normativa del Esquema Nacional de Seguridad.

D.5) HERRAMIENTAS DE COPIAS DE SEGURIDAD

El sistema o herramientas seleccionadas para realizar las copias de seguridad deben permitir la realización de copias de seguridad para los sistemas operativos involucrados en los servicios del Ayuntamiento objeto de alcance del SGSI.

Se mantendrá un contrato de mantenimiento con el proveedor o fabricante, o sistema de copia auxiliar, que asegure su disponibilidad en un tiempo máximo determinado.

Se debe guardar registro de copias realizadas con éxito, registrando la fecha y hora de la misma.

Se debe guardar registro asimismo de intentos de copias fallidos, registrando la fecha y hora de los mismos y el mensaje de error por el que no se ha procedido a realizar la misma, o bien no se ha concluido con éxito.

D.6) PRUEBAS DE RESTAURACIÓN

Cada 6 meses se realizará por parte del departamento de sistemas, el procedimiento de restauración de información para comprobar que, en caso de fallo, una copia de seguridad puede devolver un sistema a un estado de funcionamiento correcto sin perder información.

E) PROCEDIMIENTO DE COPIAS DE SEGURIDAD (BACKUP)

Los equipos y dispositivos para la realización de copias de seguridad se encuentran ubicados en el CPD del edificio principal del Ayuntamiento.

Las copias de seguridad se realizan diaria y semanalmente, siguiendo una planificación que está establecida en el apartado “Planificación” de este procedimiento. Se podrán realizar copias adicionales, siempre que ocurra una situación de riesgo que aconseje realizarlas.

Esta planificación será revisada cada vez que haya un cambio en cualquiera de los elementos que intervienen en la copia de seguridad (sistemas, soportes, herramienta de backup, etc.) así como cuando ocurra una variación importante en la cantidad de información a copiar. En especial se monitorizará la capacidad de los soportes usados y se volverá a planificar cuando se encuentre cerca de su límite.

Las copias de seguridad se realizan, a nivel de máquina y sobre las plataformas de XXXX y XXXX, con la herramienta EBACKUP, la cual realiza snapshots de las máquinas virtualizadas.

No se realizan backup del contenido de los PCs físicos.

En general se deberán tener en consideración los siguientes aspectos:

- Si se va a realizar un backup que destruya la información previa del soporte en lugar de añadir una nueva a la ya existente, se debe asegurar que la anterior se puede eliminar, bien con confidencialidad, bien conforme a la normativa de protección de datos.
- Se comprobará que el volumen de información a copiar sea menor que la capacidad del soporte a usar.

- A la finalización de la copia de seguridad, se comprobará el registro de log de la herramienta de backup para verificar si se ha realizado correctamente. En caso de existir algún error, se llevarán a cabo las siguientes acciones:
    - Se investigará, de inmediato, la causa de los errores encontrados (fallo de la herramienta, del grabador, del propio sistema) y se pondrán los medios para que no vuelva a suceder.
    - Se volverá a programar el mismo backup cuanto antes o se realizará de inmediato, a ser posible, salvo que su periodicidad sea pequeña y se considere que no incurre en un riesgo considerable al esperar a la siguiente copia planificada.
    - Se registrará la incidencia.
- Para las copias que se saquen a un soporte, se etiquetará dicho soporte o se actualizará su etiqueta si ya dispone de ella.
- Se actualizará el inventario de activos.

E.1) PROCEDIMIENTO DE COPIAS DE SEGURIDAD (BACKUP)

La planificación de las copias de seguridad comprende:

- Sistemas a copiar (información y aplicativos, incluido Sistema Operativo).
- Origen de la información (lugar donde se encuentra).
- Destino en el que se realiza la copia.
- Periodicidad, día y horarios programados en los que se realiza la copia.
- Tipo de copia (total, incremental, diferencial, etc.).

E.2) PLANIFICACIÓN DE LAS COPIAS DE SEGURIDAD

El Ayuntamiento usa una solución de virtualización compuesta por XXXX y XXXX. El sistema de copias de seguridad centraliza este proceso mediante políticas de copias donde se establece la forma y tiempo en que se realizan las copias.

La planificación de las copias de seguridad se realiza como se expone a continuación:

- Diariamente se realiza una copia de seguridad de los servidores del CPD. La copia está programada los sábados a las 22:00 horas.
- Semanalmente se realiza copia remota de los servidores existentes en el CPD del Ayuntamiento en las instalaciones de la oficina, en la cabina de almacenamiento secundaria. La copia está programada los sábados a las 22:00 horas.

Las siguientes tablas contienen el detalle del proceso de planificación.

	NAS			
Diaria	Elemento	Tipo/Contenido	Ventana	Notas
Mensual	Elemento	Tipo/Contenido	Ventana	Notas

	Cabina			
Diaria	Elemento	Tipo/Contenido	Ventana	Notas

Mensual	Elemento	Tipo/Contenido	Ventana	Notas

F) PROCEDIMIENTO DE RESTAURADO DE LA INFORMACIÓN

- Las peticiones de restauración deben ser realizadas por el propietario o el Responsable de Seguridad, bien por el Responsable del área/departamento o bien por el propio interesado, siempre que la información contenida en el backup sea de su máquina.
- El restaurado se realizará en el mismo servidor donde está el archivo origen, o en su defecto en un servidor con el mismo sistema operativo que el original al que pertenece dicho archivo origen.
- No se sobrescribirá nunca el archivo origen. Se habilitará una carpeta raíz, en la que se restaurarán los archivos, de manera que se mantenga toda la estructura del camino original.
- Se comprobará el archivo de registro log de la herramienta de restaurado, para comprobar que el mismo ha sido realizado con éxito.
- Se pueden dar dos casos:
    - **Si se trata de una Prueba de Restaurado:** se comprobará su correcta ejecución, en modo lectura, de todos los archivos restaurados, cuando no sean excesivos (10 o menos) o de una selección de ellos cuando se trate de un restaurado completo o de gran cantidad de archivos. En este segundo caso, se intentará seleccionar archivos de distintas carpetas y/o sistemas del restaurado realizado.
    - **Si se trata de un Restaurado debido a una Incidencia:** se comprobará que toda la información afectada por la incidencia se ha recuperado perfectamente en la carpeta de pruebas. Posteriormente se copiará a la localización original y se volverán a realizar las comprobaciones.
- Una vez realizadas las comprobaciones, los archivos generados por la prueba de restaurado se eliminarán de la carpeta temporal creada.
- Si el resultado ha sido incorrecto, ejecutar otra copia anterior para corregir el fallo.

F.1) PROCEDIMIENTO DE RESTAURADO DE LA INFORMACIÓN DEBIDO A UNA INCIDENCIA

En el caso de que los datos a restaurar incluyan datos de carácter personal, se deberá contar con la autorización del Responsable de la Información antes de proceder al restaurado. Se realizarán los siguientes pasos:

- Comunicar la incidencia.
- Comprobar la disponibilidad de la información a recuperar en su ubicación.
- Solicitar autorización para realizar el restaurado por correo electrónico interno.
- Realizar la restauración:
    - Definir procedimiento

G) RESPONSABLE DEL PROCEDIMIENTO

Será responsabilidad del Administrador de Seguridad velar por el cumplimiento de la presente normativa, bajo la supervisión del Responsable de Seguridad.

H) 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.
- Procedimiento de Copias de Seguridad (backup)
- Procedimiento de Restaurado de Información

I) REGISTROS/ANEXOS