NORMATIVA

GESTIÓN DE ACTIVOS

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.01	DOCUMENTO:	NORMATIVA DE GESTIÓN DE ACTIVOS

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

El presente documento describe la normativa a cumplir por el Ayto. de Baeza (en adelante Ayuntamiento) referente a la Gestión de Activos de Información.

En dicha normativa se establecen las responsabilidades y compromisos a adquirir por los usuarios, tanto externos como internos, intervinientes en el proceso.

2) ALCANCE

Esta normativa es de aplicación y obligado cumplimiento por todo el personal del Ayuntamiento, que de manera permanente o puntual, preste sus servicios a la entidad, incluyéndose en este ámbito tanto a personal fijo como personal eventual.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de Seguridad, Responsable del Sistema, Responsables de los Servicios 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

Responsable de los servicios: tendrán la responsabilidad de garantizar que se realiza la identificación e inventariado de los activos.

Responsable del inventario: tendrá la responsabilidad de realizar, mantener y actualizar los inventarios de los activos del Ayuntamiento. El responsable de seguridad podrá delegar esta función.

Responsable de activos: cada activo tendrá un responsable que será el que garantice el correcto funcionamiento del mismo y garantice que se cumplen las medidas de seguridad establecidas.

4) DESARROLLO NORMATIVO

4.1) IDENTIFICACIÓN E INVENTARIADO DE ACTIVOS

Para poder establecer las medidas de protección adecuadas a los activos, es necesario conocer los que son, qué contienen, su valor y características, dónde están situados y cómo se relacionan entre sí.

Los procesos llevados a cabo y servicios, a estos efectos, se tratarán como activos en sí mismos, que a su vez hacen uso de otros activos.

El Ayuntamiento debe tener un conocimiento de los activos que posee como parte muy importante de la administración de riesgos. Estos activos suelen dividirse en:

- **Información y Datos:** aquellos datos que deben ser preservados frente a lectura, modificación o borrado malintencionado.
- **Servicios:** prestados a la ciudadanía o de manera interna a las diferentes áreas del Ayuntamiento.
- **Sistemas:** que soportan los servicios en cuanto a que es preciso preservar su integridad física, lógica y su configuración, ya que de ello depende el buen funcionamiento de aquellos.

Se mantendrá un inventario de los activos, preferiblemente automatizado, en el que queden registrados los datos necesarios para localizar tanto lógica como físicamente, todos y cada uno de los activos.

El inventario de activos, asimismo, reflejará para cada uno ellos, al menos: características principales, valor, clasificación, información que contienen, y la relación y dependencias que poseen con otros activos de su entorno.

4.2) CLASIFICACIÓN

Los activos de información del Ayuntamiento deben ser clasificados conforme a las categorías estipuladas en el Esquema Nacional de Seguridad y en cada una las dimensiones de seguridad (Disponibilidad, Trazabilidad, Integridad, Confidencialidad y Autenticidad), según proceda.

Las valoraciones de los sistemas de información deben estar centradas en aquellos activos y en aquellas dimensiones en las que el impacto de un incidente sea mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante. Cuando el sistema trate datos de carácter personal, se garantizará una seguridad adecuada mediante medidas técnicas y organizativas apropiadas tras la evaluación de los resultados del análisis del riesgo, haciendo especial hincapié para datos catalogados como de categoría especial o relativos a condenas e infracciones penales (RGPD (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de Derechos Digitales).

El Anexo A – Criterios de valoración de Servicios e Información conforme al ENS recoge los criterios de valoración empleados por el Ayuntamiento.

4.2.1) ETIQUETADO

Cada activo tendrá asignado un nombre o número de referencia físico que lo identifique unívocamente. Se seguirán las directrices del procedimiento “PR.01. Etiquetado y Clasificación de activos e información”.

Cuando el activo esté situado en un área de acceso restringido y/o no se comprometa su seguridad, se etiquetará con su nombre o referencia de forma físicamente visible. Cuando a un activo se le pueda asignar un nombre lógico, se hará, y será el mismo que tiene asignado físicamente.

4.2.2) RESPONSABLE

Se designará a un responsable del inventario, que velará por su correcto mantenimiento y actualización. En la medida de lo posible se utilizará una herramienta mecanizada que facilite la gestión de dicho inventario.

4.2.3) RESPONSABLE DE ACTIVOS

Cada uno de los activos tendrá asignado un Responsable. Esta persona tendrá la responsabilidad última de velar continuamente por el correcto estado, uso y seguridad del activo, y tomará las decisiones sobre él.

Cuando resulte adecuado, la propiedad se puede asignar sobre un grupo de activos estrechamente relacionados entre sí por alguna circunstancia (por ejemplo, un determinado servicio que es proporcionado por varios activos). En este caso el responsable lo será de todos los activos que intervienen.

Las funciones y responsabilidades del responsable del activo son las siguientes:

- Garantizar las instrucciones o condiciones físicas, lógicas y de seguridad en las que debe mantenerse el activo, así como sus usos.
- Realizar comprobaciones periódicas las condiciones y usos del activo.

Estas funciones podrán ser delegadas en otras personas, aunque la responsabilidad última sobre el activo siempre permanecerá en su Responsable.

4.2.4) GESTOR DEL ACTIVO

Cuando sea necesario, adicionalmente al Responsable, se asignará una persona como Gestor del activo, que llevará a cabo las funciones técnicas propias de gestión y mantenimiento del activo necesarias para su correcto estado y/o funcionamiento y seguridad.

Las funciones del gestor son las siguientes:

- Realizar las gestiones y ejecutar las acciones necesarias sobre el activo en cada momento, para su correcto estado, mantenimiento, uso y seguridad, atendiendo a las especificaciones de los fabricantes en cuanto a la instalación y mantenimiento de los mismos.

- Asegurar que todas aquellas acciones que afecten al activo se llevan a cabo conforme a las instrucciones del Responsable.
- Obtener aprobación del Responsable para los cambios necesarios en el activo.
- Comunicar dichos cambios al responsable del inventario y demás responsables que pudiesen verse afectados por éstos.
- Llevar a cabo aquellas otras funciones que el Responsable le delegue.

En caso de que no se haya considerado necesario la designación de esta figura, todas las funciones serán asumidas por el Responsable del Activo.

5) RESPONSABLE DEL CUMPLIMIENTO

Será función del Responsable de Seguridad velar por el cumplimiento de lo descrito en esta normativa y revisar su correcta aplicación.

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.

Normativa Interna/Procedimientos

- PR.01. Etiquetado y Clasificación de activos e información.

7) REGISTROS/ANEXOS

ANEXO 1: CRITERIOS PARA LA VALORACIÓN DE LAS DIMENSIONES DE LOS SERVICIOS

CRITERIOS COMUNES

Nivel ALTO

- **Disposición legal o administrativa.** Por disposición legal o administrativa (ley, decreto, orden, reglamento…).
- **Perjuicio Directo al ciudadano.** Grave daño, de difícil o imposible reparación al ciudadano.
- **Incumplimiento de una Norma:**
  - **Legal.** Incumplimiento grave de una norma jurídica.
  - **Regulatoria.** Implica sanción grave de un regulador y/o pérdida de licencia de operar.
  - **Contractual.** Incumplimiento grave de una obligación contractual.
  - **Interna.** Incumplimiento grave de una norma interna.
- **Pérdidas económicas.** Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización).
- **Reputación.** Daño reputacional grave con los ciudadanos o con otras organizaciones.
- **Protestas.** Protestas masivas (alteración seria del orden público).

- **Delitos.** Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Nivel MEDIO

- **Disposición legal o administrativa.** Por disposición legal o administrativa (ley, decreto, orden, reglamento…).
- **Perjuicio Directo al ciudadano.** Daño importante, aunque subsanable al ciudadano.
- **Incumplimiento de una Norma:**
    - **Legal.** Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable.
    - **Regulatoria.** Implica sanción significativa de un regulador.
    - **Contractual.** Incumplimiento material o forma de una obligación contractual.
    - **Interna.** Incumplimiento material o formal de una norma interna.
- **Pérdidas económicas.** Pérdidas económicas importantes (igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización).
- **Reputación.** Daño reputacional importante con los ciudadanos o con otras organizaciones.
- **Protestas.** Protestas públicas (alteración del orden público).
- **Delitos.** Favorecería significativamente la comisión de delitos o dificultaría su investigación.

Nivel BAJO

- **Disposición legal o administrativa.** Por disposición legal o administrativa (ley, decreto, orden, reglamento)..
- **Perjuicio Directo al ciudadano.** Algún perjuicio al ciudadano.
- **Incumplimiento de una Norma:**
    - **Legal.** Incumplimiento formal leve de una norma jurídica, de carácter subsanable.
    - **Regulatoria.** Implica incumplimiento de normativa de un regulador.
    - **Contractual.** Incumplimiento leve de una obligación contractual.
    - **Interna.** Incumplimiento leve de una norma interna.
- **Pérdidas económicas.** Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización).
- **Reputación.** Daño reputacional apreciable con los ciudadanos o con otras organizaciones.
- **Protestas.** Múltiples protestas individuales..
- **Delitos.** Favorecería la comisión de delitos.

NO ADSCRITOS.

- **Disposición legal o administrativa.** No existe ninguna disposición legal que condicione su nivel.
- **Perjuicio Directo al ciudadano.** No supone ningún perjuicio directo al ciudadano.
- **Incumplimiento de una Norma:**
    - **Legal.** No implica incumplimiento de una norma jurídica.
    - **Regulatoria.** No implica incumplimiento de normativa de un regulador.
    - **Contractual.** No implica incumplimiento de una obligación contractual.
    - **Interna.** No implica incumplimiento de normativa interna.
- **Pérdidas económicas.** No implica pérdidas económicas.
- **Reputación.** No implica daño reputacional.
- **Protestas.** No se prevé que pueda desembocar en protestas.
- **Delitos.** No facilitaría la comisión de delitos ni dificultaría su investigación.

CRITERIOS ESPECÍFICOS

DISPONIBILIDAD

Nivel ALTO

- **Tiempo Objetivo de Recuperación.** La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas.

Nivel MEDIO

- **Tiempo Objetivo de Recuperación.** La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día.

Nivel BAJO

- **Tiempo Objetivo de Recuperación.** La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días.

NO ADSCRITOS

- **Tiempo Objetivo de Recuperación.** La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días.

ANEXO 2: CRITERIOS PARA LA VALORACIÓN DE LAS DIMENSIONES DE LA INFORMACIÓN

CRITERIOS COMUNES

Nivel ALTO

- **Disposición legal o administrativa.** Por disposición legal o administrativa (ley, decreto, orden, reglamento…).
- **Perjuicio Directo al ciudadano.** Grave daño, de difícil o imposible reparación al ciudadano.
- **Incumplimiento de una Norma:**
  - **Legal.** Incumplimiento grave de una norma jurídica.
  - **Regulatoria.** Implica sanción grave de un regulador y/o pérdida de licencia de operar.
  - **Contractual.** Incumplimiento grave de una obligación contractual.
  - **Interna.** Incumplimiento grave de una norma interna.
- **Pérdidas económicas.** Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización).
- **Reputación.** Daño reputacional grave con los ciudadanos o con otras organizaciones.
- **Protestas.** Protestas masivas (alteración seria del orden público).
- **Delitos.** Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Nivel MEDIO

- **Disposición legal o administrativa.** Por disposición legal o administrativa (ley, decreto, orden, reglamento…).
- **Perjuicio Directo al ciudadano.** Daño importante, aunque subsanable al ciudadano.
- **Incumplimiento de una Norma:**
  - **Legal.** Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable.
  - **Regulatoria.** Implica sanción significativa de un regulador.
  - **Contractual.** Incumplimiento material o forma de una obligación contractual.
  - **Interna.** Incumplimiento material o formal de una norma interna.
- **Pérdidas económicas.** Pérdidas económicas importantes(igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización).
- **Reputación.** Daño reputacional importante con los ciudadanos o con otras organizaciones.
- **Protestas.** Protestas públicas (alteración del orden público).
- **Delitos.** Favorecería significativamente la comisión de delitos o dificultaría su investigación.

Nivel BAJO

- **Disposición legal o administrativa.** Por disposición legal o administrativa (ley, decreto, orden, reglamento)..
- **Perjuicio Directo al ciudadano.** Algún perjuicio al ciudadano.
- **Incumplimiento de una Norma:**
  - **Legal.** Incumplimiento formal leve de una norma jurídica, de carácter subsanable.
  - **Regulatoria.** Implica incumplimiento de normativa de un regulador.
  - **Contractual.** Incumplimiento leve de una obligación contractual.
  - **Interna.** Incumplimiento leve de una norma interna.
- **Pérdidas económicas.** Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización).
- **Reputación.** Daño reputacional apreciable con los ciudadanos o con otras organizaciones.
- **Protestas.** Múltiples protestas individuales..
- **Delitos.** Favorecería la comisión de delitos.

NO ADSCRITOS.

- **Disposición legal o administrativa.** No existe ninguna disposición legal que condicione su nivel.
- **Perjuicio Directo al ciudadano.** No supone ningún perjuicio directo al ciudadano.
- **Incumplimiento de una Norma:**
  - **Legal.** No implica incumplimiento de una norma jurídica.
  - **Regulatoria.** No implica incumplimiento de normativa de un regulador.
  - **Contractual.** No implica incumplimiento de una obligación contractual.
  - **Interna.** No implica incumplimiento de normativa interna.

- **Pérdidas económicas.** No implica pérdidas económicas.
- **Reputación.** No implica daño reputacional.
- **Protestas.** No se prevé que pueda desembocar en protestas.
- **Delitos.** No facilitaría la comisión de delitos ni dificultaría su investigación.

CRITERIOS ESPECÍFICOS

Nivel ALTO

No es aplicable.

Nivel MEDIO

- **Cantidad considerable de datos personales.** Operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y extrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala.
- **Importante riesgo para los derechos y libertades de interesados.** Operación de tratamiento que entraña un alto riesgo para los derechos y libertades de los interesados, en particular cuando esta operación hace más difícil para los interesados el ejercicio de sus derechos.
- **Evaluación sistemática y exhaustiva de aspectos personales.** Operación de tratamiento para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas.
- **Control de zonas de acceso público a gran escala.** Operaciones de control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos.

Nivel BAJO

No es aplicable.

NO ADSCRITOS.

No es aplicable.

---

[1] RTO (*Recovery Time Objetive):* Tiempo de Recuperación del Servicio