NORMATIVA

EXPLOTACIÓN

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.26	DOCUMENTO:	NORMATIVA DE EXPLOTACIÓN

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

Este documento establece la Normativa de Explotación, en el ámbito de los Sistemas de Información del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento), persiguiendo garantizar la correcta operación, administración y funcionamiento de los sistemas de procesado de la información.

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

El responsable de la puesta en marcha de las medidas descritas en la presente normativa será el Responsable de Seguridad, que velará en todo momento por que el cumplimiento de lo referente en esta normativa junto con el Responsable de los Sistemas de la información.

4) DESARROLLO NORMATIVO

4.1) SEPARACIÓN DE FUNCIONES

El procedimiento de segregación de tareas permite realizar un control de las actividades que se realizan en el sistema y reducir las modificaciones no intencionadas o no autorizadas de la información almacenada en los mismos.

Tal y como se ha indicado anteriormente, y debido a la limitación en el número de administradores de los sistemas, se definen los controles que suplen a la segregación de tareas allí donde sea factible.

Para sustituir la segregación de tareas en la administración de sistemas se han documentado los controles que se siguen para el registro de auditoría de las actividades realizadas en los sistemas tanto por usuarios administradores como por usuarios normales del sistema, actividades de monitorización del uso de los sistemas, protección de los registros de auditoría, etc.

Se define la responsabilidad de revisión de los informes de auditoría de usuarios administradores al Responsable del Seguridad, el cual se encargará de comprobar que en los informes recibidos no se detectan actividades sospechosas o no intencionadas de acceso a información debidas a tareas realizadas por el Responsable del Sistema.

A continuación, mostramos los distintos perfiles que intervienen, así como las funciones y responsabilidades y medidas.

Comité de Seguridad	Gestionar y coordinar proactivamente la seguridad de la información.
Responsable de la Información	Tiene potestad para aprobar los requisitos de una información en materia de seguridad.. Podrá convocar las reuniones del Comité. Es el responsable directo de ejecutar las medidas adoptadas por el Comité.
Responsable de Seguridad	Asesorar en materia de seguridad. Tendrá potestad para determinar los requisitos técnicos de seguridad de la información y de los servicios. Informará del estado de la seguridad en el área de sistemas de la información. Podrá convocar al Comité de Seguridad y remitir información y comunicados a los miembros del Comité.
Responsable del Sistema	Vigilar el cumplimiento de las normas de seguridad dentro de su área e informar al

	Responsable de la Información del cumplimiento de la normativa de seguridad aprobada por el el Comité de Seguridad.
Responsable de la Entidad	Es el responsable de la explotación del Ayuntamiento, estableciendo requisitos, fines y medios para la realización de dicha tarea. Vigilar el cumplimiento de las normas de seguridad definidas en su entidad. Informar del cumplimiento de la normativa de seguridad.

4.2) SEPARACIÓN DE ENTORNOS

Cuando proceda, los entornos de Desarrollo, Prueba y Producción, incluyendo aplicaciones e información, y siempre que sea posible, estarán separados preferentemente de manera física, y se definirán y documentarán las reglas para mover el software entre los diferentes entornos.

- No se debe tener acceso desde Producción a las herramientas de desarrollo y pruebas.
- Separar las actividades de desarrollo y pruebas en entornos separados.
- No se debe tener acceso desde el entorno de Desarrollo a los datos de Producción.
- Utilizar sistemas de autenticación y autorización independientes para los diferentes entornos, así como diferentes perfiles de acceso a los mismos.
- Los datos e información real de Producción de tipo sensible o confidencial, así como los datos de carácter personal no podrán ser copiados y procesados en el entorno de Preproducción a no ser que sea imprescindible y siempre que se hayan establecido las mismas medidas de seguridad que para el entorno de Producción.
- Todo software o sistema de información debe ser probado en un entorno de Preproducción antes de instalarse en Producción. Se realizarán las pruebas necesarias para garantizar que el nuevo componente no introduce vulnerabilidades de seguridad, funciona de forma acorde a los requerimientos, no afecta a la operación del sistema de forma adversa y no realiza cambios no autorizados en el sistema.

4.3) PLANIFICACIÓN DE LA CAPACIDAD Y LOS RECURSOS

Para minimizar el riesgo de fallos en los sistemas y garantizar su disponibilidad y correcto funcionamiento y eficacia se llevarán a cabo las acciones necesarias para gestionar la capacidad y los recursos eficientemente, para ello:

- Se monitorizarán los sistemas y servicios de forma continua, midiendo y revisando el uso de los recursos.
- Se planificarán las ampliaciones necesarias y/o nuevos sistemas en base a las necesidades futuras del Ayuntamiento.
- Se implementarán controles que avisen ante posibles fallos a corto y medio plazo, y así evitar “cuellos de botella”, sobre todo en los sistemas más críticos.
- Se activará algún mecanismo de alarma en tiempo real y aviso por mail que alerte de deficiencias en las capacidades de los equipos más críticos.

4.4) CUENTAS DE USUARIO, AUTENTICACIÓN Y ACCESO AL SISTEMA

Se establecerán las especificaciones concretas a cumplir para la gestión, asignación y distribución de las cuentas de usuario y sus contraseñas asociadas conforme a la Normativa de Gestión de Cuentas y Proceso de Autorización de Acceso.

En lo relativo a la configuración del sistema con respecto a las cuentas de usuario y contraseñas se observarán los siguientes requerimientos:

- Las contraseñas no deben mostrarse en claro por pantalla y siempre se almacenarán de manera cifrada en el sistema (preferiblemente cifrado no reversible).
- No se mostrará información relativa al sistema en la fase de autenticación de un usuario. En el caso de que falle la autenticación del mismo, no debe proporcionarse información sobre la parte de la secuencia que ha fallado.
- Se procederá al bloqueo de la cuenta ante cinco intentos reiterados de acceso al sistema, guardándose registro de ello.

- Se guardarán en los registros del sistema las trazas (logs) de los accesos de los usuarios, detallando en las mismas el identificador del usuario y la fecha y hora de acceso y, en el caso de datos personales de categoría especial, el tratamiento accedido, el tipo de acceso y si ha sido autorizado o denegado.
- Se deshabilitarán las cuentas de invitado, en caso de existir, así como también se modificarán las contraseñas por defecto de los sistemas.
- Cada persona deberá acceder al sistema con su cuenta de usuario personal, con sus privilegios asignados y estrictamente necesarios para el desarrollo de sus funciones dentro del Ayuntamiento.
- Siempre que no se esté utilizando la consola de administración del sistema, ésta deberá permanecer bloqueada con una contraseña, así como los accesos remotos, mediante Terminal Server o similar, deberán bloquearse cerrar la sesión cuando no se esté administrando remotamente.

4.5) REGISTRO DE ACTIVIDADES DEL PERSONAL DE OPERACIÓN Y ADMINISTRACIÓN

Deberá registrarse las actividades realizadas por el personal de operación y administración de sistemas tales como:

- Identificación del usuario.
- Tiempos de inicio y cierre de los sistemas.
- Errores de los sistemas.
- Intentos de acceso a sistemas, a información crítica o a acciones restringidas.
- Ejecución de operaciones críticas.
- Cambios o modificaciones en la información crítica.

4.6) SOFTWARE

Las medidas de seguridad a tener en cuenta respecto al software serán las siguientes:

- Queda prohibido la instalación de software no autorizado por Ayuntamiento.
- Queda prohibido la instalación de software sin licencia o, en caso de tratarse de software de dominio público, deberá haberse obtenido de una fuente fiable.
- Con objeto de evitar agujeros de seguridad publicados y conocidos por intrusos, los sistemas operativos de base deberán mantenerse actualizados a la última versión, siempre que no implique efectos secundarios inadecuados.
- No se instalarán versiones “beta” de ningún software en los entornos de Preproducción o Producción, a no ser que sea expresamente recomendado por el fabricante.
- Al igual que el equipamiento, todo aquel software cuyo coste o necesidad de disponibilidad lo justifique, deberá estar protegido con un contrato de mantenimiento y actualización de versiones, que permita la actualización periódica por el proveedor o fabricante, tanto de parches de seguridad como de nuevas versiones de productos. Cuando este tipo de contrato no sea posible, el personal de administración y operación se suscribirá o consultará listas, foros o fuentes de información que le mantenga informado de actualizaciones respecto a dicho software.

4.6.1) CONTROLES CONTRA SOFTWARE MALICIOSO

El Responsable de Seguridad definirá los controles de detección y prevención para la protección contra software malicioso y desarrollará procedimientos adecuados de concienciación de usuarios en materia de seguridad.

Entre los controles a implantar se encuentran:

- Instalar y actualizar periódicamente software de detección y desinfección de virus, examinando los equipos y medios informáticos, como medida preventiva y rutinaria. Se instalarán agentes gestionados de manera centralizada.
- Realizar escaneos periódicos en busca de virus.
- Verificar, antes de su uso, la presencia de virus en archivos o medios electrónicos de origen desconocido, o en archivos recibidos del exterior, bien a través de correo electrónico, bien a través de Internet.
- Concienciar a los usuarios acerca de los virus, de los falsos virus, de sus consecuencias y de cómo proceder frente a los mismos.

4.7) SERVICIOS Y PROCESOS

- En cada sistema permanecerán habilitados única y exclusivamente los servicios que se identifiquen como necesarios para las funciones que le correspondan.
- Deberá elaborarse un documento que describa los servicios que deben figurar en cada sistema además de los necesarios para las tareas de administración.
- Se establecerá un control periódico de los servicios que deben estar arrancados en cada sistema.
- Los procesos correspondientes a las aplicaciones de los sistemas serán lanzados con usuarios que tengan los mínimos privilegios necesarios para su correcto funcionamiento.

4.8) COPIAS DE SEGURIDAD

Se definirá, conforme a la Normativa de Copias de Seguridad (Backup), la planificación de copias de seguridad, en la que se incluirán todos los sistemas, con la periodicidad correspondiente, de forma que se garantice la recuperación de los mismos y la de los servicios que soportan a la mayor brevedad posible.

4.9) AUDITORÍA

Para la configuración de la auditoría de los sistemas en producción se seguirá lo establecido en la Normativa de Auditorías y Registro de los Sistemas.

4.10) DOCUMENTACIÓN DE LOS SISTEMAS

Toda documentación sobre operación, administración y mantenimiento de sistemas, tales como manuales, procedimientos, configuraciones, etc. debe ser adecuadamente protegida:

- Toda la documentación generada tendrá asignado un responsable, que por defecto será el Responsable de Seguridad, que velará por su cumplimiento, mantenimiento y actualización. El responsable y la versión del documento estará impresa en el mismo.
- La documentación impresa será almacenada en lugar de acceso restringido.
- El personal de operación, mantenimiento y administración tendrá acceso solamente a la documentación necesaria para el correcto desempeño de sus funciones.
- Se deberá mantener copias de seguridad de la documentación.

4.11) GESTIÓN DE CAMBIOS Y VERSIONES

Los cambios, actualizaciones de versiones y paso a producción o explotación de servicios o sistemas se llevarán a cabo a través de procesos formales que deberán estar definidos y documentados. El proceso, que puede ser común a todos los sistemas, debe estar aprobado por el Responsable del Sistema.

No se realizarán cambios significativos (mayores y/o medios) sin la correspondiente aprobación del Responsable del Sistema o en quien él delegue. Se entenderá cambio significativo aquellos que tienen un gran impacto.

El Responsable de Seguridad controlará además que los cambios no afecten a la seguridad de los sistemas ni a la información que soportan, evaluando el posible impacto operativo de los cambios previstos y verificando su correcta implementación.

4.11.1) FUNCIONES DEL RESPONSABLE DE GESTIÓN DE CAMBIOS Y VERSIONES

Las funciones del Responsable de Gestión de Cambios y Versiones deberán ser al menos las siguientes:

- Revisar y aprobar o rechazar los cambios.
- Establecer, junto con el solicitante, la prioridad y categoría del cambio.
- Analizar la viabilidad del cambio. Convocar cuando sea necesario al Responsable del Sistema, Responsable de Seguridad y cualquier otra figura relevante, para evaluar y decidir sobre el cambio.
- Decidir sobre las particularidades de los cambios urgentes.
- Recibir las opiniones sobre los cambios realizados, realizar revisiones e implementar mejoras en el proceso de gestión de cambios y versiones.

4.11.2) FUNCIONES DEL RESPONSABLE DEL SISTEMA EN RELACIÓN CON LOS CAMBIOS

- Mantener un registro de los cambios aceptados y su fecha de ejecución.

- Enviar las solicitudes de cambios a los grupos de implementación y prueba adecuados en cada caso, dimensionando el número de recursos necesarios para ello.
- Comprobar la correcta ejecución de los cambios y cerrarlos.
- Elaborar y presentar informes periódicos del proceso.

4.12) OPERACIÓN Y MANTENIMIENTO POR TERCEROS

4.12.1) IDENTIFICACIÓN DE RIESGOS DEL ACCESO DE TERCERAS PARTES

Previamente a proporcionar acceso a terceras partes a información del Ayuntamiento, el Responsable de Seguridad y el Responsable del Sistema afectado llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta:

- Tipo de acceso requerido (físico, lógico, y a qué recurso).
- Periodo de acceso.
- Motivos que solicitan el acceso.
- El valor de la información accedida.
- Controles de seguridad empleados por el tercero.
- Posibles incidencias de este acceso en la seguridad del Ayuntamiento.

En todos los contratos cuyo objeto sea la prestación de servicios bajo cualquier modalidad jurídica, que deban desarrollarse dentro del Ayuntamiento, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se proporcionará acceso a terceros a la información, a las instalaciones de procesado (Centro de Proceso de Datos o CPD) u otras áreas de servicios críticos, hasta que se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso a los mismos.

4.12.2) TÉRMINOS DE LA CONTRATACIÓN

Siempre que se lleve a cabo la contratación de obras o servicios con empresas o terceras personas que supongan el acceso a la información del Ayuntamiento, se llevarán a cabo previamente las siguientes acciones:

- Comprobación de las referencias y experiencias indicadas por la empresa oferente en cuanto a otras obras y servicios similares en otros clientes.
- Investigar posibles antecedentes de la empresa en cuanto a incumplimientos o irregularidades anteriores.
- Incluir, salvo que no procedan en cada caso concreto, cláusulas específicas de seguridad en el contrato, tales como:
    - De Confidencialidad, en la que se indique el deber de guardar secreto profesional sobre cualquier información a la que tenga acceso, incluso tras la finalización de la relación laboral. Esto deberá exigirse para posibles subcontrataciones.
    - La obligación del cumplimiento de las normas y procedimientos de seguridad establecidas en el Ayuntamiento.
    - La obligación de comunicar las incidencias de seguridad detectadas que comprometan los bienes del Ayuntamiento.
    - La protección del equipamiento, soportes e información en las dependencias de terceros y/o en su traslado.
    - En el caso de existir tratamiento de datos personales se incluirán en el contrato las cláusulas estipuladas para dar cumplimiento al art. 28 del RGPD (UE) 2016/679.
    - Se incluirá acuerdos de nivel de servicios con los niveles de servicio mínimos a obtener, definiéndose además los controles de seguridad aplicables y las normas y procedimientos de operación y seguridad a cumplir.
    - Derecho a auditar responsabilidades contractuales o surgidas del contrato.
    - La devolución, a la finalización de la relación laboral, de toda la información y equipamiento del Ayuntamiento en poder del tercero.
    - Restricciones a la copia y divulgación de toda información perteneciente y concerniente al Ayuntamiento, así como lo relativo a los derechos de Propiedad Intelectual.

    - Responsabilidades relativas a la instalación y mantenimiento de hardware y software.
- Incluir, según necesidad, los siguientes controles
    - Acuerdos de control de acceso que contemplen:
        - Métodos de acceso permitidos.
        - Proceso de autorización de acceso y privilegios de usuario.
        - Requerimientos para mantener actualizada una lista de usuarios autorizados a utilizar los servicios y sus derechos y privilegios con respecto a dicho uso.
    - Procedimiento claro y detallado de la gestión y administración de cambios.
    - Métodos y procedimientos de formación a usuarios y administradores en materia de Seguridad de la Información.
    - Controles que garanticen la protección contra software malicioso.
    - Métodos empleados para mantener la disponibilidad de los servicios ante la ocurrencia de desastres.

4.12.3) OUTSOURCING

En caso de outsourcing se deberá tener en cuenta, además:

- La forma de transmisión de la información y conocimientos necesarios durante el proceso.
- La información que debe permanecer en el Ayuntamiento debido a su criticidad.
- Establecimiento de controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
- Prever y acordar los pasos necesarios para la recuperación de la información a la finalización del contrato.
- Derechos de auditoría por parte del Ayuntamiento, de forma directa o a través de un tercero subcontratado por el organismo.

4.12.4) RESPONSABILIDAD

Cualquiera que sea el grado de externalización del servicio u operaciones, se nombrará uno o varios responsables de los servicios externalizados del Ayuntamiento, como responsables de monitorizar y velar por el cumplimiento de los niveles de servicio y seguridad acordados.

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.
- Normativa de Gestión de Cuentas y Proceso de Autorización de Acceso.

7) REGISTROS/ANEXOS