NORMATIVA

MANTENIMIENTO DEL SOFTWARE EN PRODUCCIÓN

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.16	DOCUMENTO:	NORMATIVA DE MANTENIMIENTO DEL SOFTWARE

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 objeto de la presente normativa es el de establecer las normas necesarias para el control de actualizaciones, parches de seguridad y cambios en el código fuente de los softwares que son propiedad del Excmo. Ayuntamiento de Baeza. (en adelante Ayuntamiento). En dicha normativa también se regulará el método de control y la sistemática a seguir en lo que se refiere a vulneraciones de seguridad.

2) ALCANCE

Esta normativa es de obligado cumplimiento para todo el personal del Ayuntamiento, en especial aquellos que se encuentran dentro del departamento/área de desarrollo. también será de aplicación a aquellos terceros (fabricantes o proveedores) que, previa autorización al efecto, tenga que acceder a los software o servidores 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.

3) RESPONSABILIDADES

El Responsable del Sistema, o la persona que este delegue, será la persona encargada de autorizar el uso del código fuente o de las actualizaciones que se requieran. Será también el encargado de velar por que se lleve un registro de actualizaciones, configuraciones y parches de seguridad. En el apartado de gestión de vulnerabilidades asegurará que al menos, con periodicidad anual, se realiza una auditoría interna y/o una prueba de penetración. Suya es la capacidad para permitir el acceso a los servidores en producción por parte de terceros.

4) DESARROLLO NORMATIVO

4.1) CONTROL DEL SOFTWARE EN PRODUCCIÓN

La actualización de software (aplicaciones, parches, librería, etc.) en los sistemas en Producción debe ser realizada por administradores experimentados y mediante el "*Procedimiento de Gestión de Cambios y Versiones*".

En el entorno de Producción solo se permitirá código ejecutable aprobado por el Responsable del área/departamento.

El código fuente debe haber sido probado previamente en un entorno diferente al de Producción.

Después de realizar cambios y actualizaciones en el sistema, incluidos los del Sistema Operativo, se probarán todas las aplicaciones críticas de éste para comprobar que dichos cambios no afectan a su correcto funcionamiento. Se actualizarán, además, los planes de continuidad que se vean afectados por dichos cambios.

Se llevará un control de las configuraciones y documentación del sistema.

Se tendrá un registro de todas las actualizaciones cambios y pasos a producción realizados en los sistemas. Estos se realizarán teniendo preparado previamente un procedimiento de marcha atrás. Las versiones antiguas de software se almacenarán para poder ser utilizadas en caso de fallos en las nuevas.

Los parches de seguridad se aplicarán cuando se reduzca o elimine una vulnerabilidad de la versión de software existente. En sistemas críticos no se llevarán a cabo actualizaciones automáticas de parches.

El acceso a los servidores en Producción por parte de los proveedores o fabricantes, estará solo permitido cuando sea estrictamente necesario para su administración o mantenimiento. Este hecho deberá ser aprobado por el Responsable del Sistema y monitorizado.

4.2) GESTIÓN DE VULNERABILIDADES TÉCNICAS

Al menos una vez al año, se realizará, una auditoría técnica de las vulnerabilidades del sistema (software base y servicios ofrecidos por los aplicativos) y pruebas de penetración (hacking ético).

Se establecerá un plan de respuesta para mitigar todas aquellas deficiencias encontradas, dando prioridad a aquellas con mayor riesgo de seguridad.

Será necesario un inventario de activos actualizado para llevar a cabo de una forma correcta la gestión de vulnerabilidades.

La gestión de las vulnerabilidades técnicas se llevará a cabo según el "*Procedimiento de Gestión de Vulnerabilidades Técnicas*".

5) RESPONSABLE DEL CUMPLIMIENTO

El Responsable del Sistema, en colaboración con el responsable de seguridad, será el encargado de velar por el cumplimiento de esta normativa.

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.
- Procedimiento de Gestión de Vulnerabilidades Técnicas.
- Procedimiento de Gestión de Cambios y Versiones.

7) REGISTROS/ANEXOS