NORMATIVA

AUDITORÍAS Y REGISTRO DE LOS SISTEMAS

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.19	DOCUMENTO:	NORMATIVA DE AUDITORÍAS Y REGISTRO DE LOS SISTEMAS

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 regular la realización de auditorías de control en los sistemas del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento) y la generación de registros y eventos que evidencien el nivel de seguridad de la entidad.

2) ALCANCE

Esta normativa es de aplicación a todos los usuarios del Ayuntamiento y afecta a todos los servicios de la entidad.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de Seguridad, Responsable de Sistemas 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 Seguridad, en consonancia con el Responsable de la Entidad, tendrán la responsabilidad de realizar las auditorías de control necesarias para el aseguramiento de los sistemas, y determinarán sobre qué eventos deberán mantenerse registros para verificar el grado de seguridad de la entidad.

4) DESARROLLO NORMATIVO

Se deberán registrar y mantener almacenados todos aquellos eventos que se consideren de interés para posibilitar tanto la detección de actividades que puedan comprometer o hayan comprometido la seguridad, como aquéllas que permitan comprobar la efectividad de los controles, las políticas de seguridad establecidas por el Ayuntamiento y los requerimientos legales aplicables. Estos registros deben permitir ser analizados periódicamente.

Los eventos a registrar se establecerán en base a los riesgos y controles de seguridad de cada uno de los sistemas y teniendo siempre en cuenta el consumo de recursos que ello supone, con el fin de evitar la degradación del sistema.

Como regla general se deben almacenar al menos los siguientes eventos, además de los específicos que requiera cada sistema:

- Activación y desactivación del proceso de registro.
- Cambios en la configuración de la auditoría del sistema.
- Cambios en las configuraciones en el sistema en sí.
- Intentos de acceso e inicios de sesión con éxito.
- Intentos de acceso fallidos.
- Cambios en los privilegios de usuario.
- Acciones que realicen los usuarios privilegiados, como el arranque y parada de servicios o del sistema, accesos a recursos críticos, etc.
- Activación/desactivación o modificación de los controles de seguridad implantados en el sistema.
- Fallos del sistema o de los servicios que presta.
- Cambios en tramites finalizados.

Para cada evento se almacenarán al menos, los siguientes datos:

- Identificación de usuario.
- Fecha y hora.
- Tipo y descripción del evento.
- Origen del evento
- Recurso sobre el que se ha realizado la acción o ha actuado el evento.

Cada registro de evento se deberá registrar acorde al Procedimiento de Auditoría y Registro (logs) del Sistema.

4.1) ALMACENAMIENTO DE REGISTROS

Además de los ficheros de registro mantenidos en el sistema, se deben guardar copias de seguridad de los mismos para evitar la pérdida de información debido al borrado accidental o deliberado de los datos.

Es recomendable que el registro se realice en un sistema a prueba de manipulación, de forma que se evite que un mal uso del sistema o un ataque pueda ser ocultado mediante la modificación de los logs.

Debe almacenarse copia de los archivos de registro ("logs") durante el tiempo indicado en la Normativa de Retención de la Información.

Se deberá tener en cuenta y monitorizar la capacidad de almacenamiento de sistema o ficheros de registro para evitar su llenado. Se establecerán si fuese necesario, rotaciones para el almacenamiento.

En el caso de que los ficheros de registro no estén disponibles o no puedan continuar guardando eventos por cualquier motivo, el sistema continuará operando normalmente y se generará una alarma que avise al responsable de la operación del sistema siempre que sea posible. Se tomarán inmediatamente las medidas oportunas para rectificar la situación lo antes posible.

4.2) ACCESO A LOS REGISTROS

El acceso a los ficheros y herramientas de registro debe estar restringido a los miembros del grupo encargado de la administración de los sistemas. El acceso a los ficheros de registro también será permitido eventualmente al equipo de desarrollo, si existe, para la depuración de errores de programas.

No estará permitido en ningún caso, incluso a los administradores, el borrado, modificación o desactivación de los registros. Se restringirá técnicamente para todos y, si el sistema lo permite, también a los administradores.

4.3) SINCRONIZACIÓN DE FECHA Y HORA

Para una correcta interpretación de la sucesión de eventos es imprescindible que el registro de estos se realice con la fecha y hora correcta, para lo cual se deberán mantener los sistemas sincronizados automáticamente con una fuente de tiempo fiable.

4.4) REVISIÓN Y CONTROL DE REGISTROS

En general, todos los registros de auditoría deben ser revisados periódicamente. Siempre que sea factible, y al menos para los sistemas más críticos, es recomendable el uso de herramientas de recolección, gestión y correlación de eventos para facilitar esta tarea, además del hecho de que éstas comunicarán los posibles problemas de seguridad casi en tiempo real.

En caso de los datos de categoría especial, la revisión deberá ser llevada a cabo, al menos, una vez cada seis meses y se elaborará un informe de las revisiones realizadas y los problemas detectados.

Todos los incidentes detectados deberán ser comunicados según la "*Normativa de Comunicación y Gestión de Incidencias*".

5) RESPONSABLE DEL CUMPLIMIENTO

Será el Responsable de Seguridad el encargado de verificar que se realizan las auditorías y se mantienen los registros definidos en la presente normativa, para cumplir fehaciente con lo dispuesto en 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.
- Normativa de Comunicación y Gestión de Incidentes.
- Procedimiento de Auditoría y Registro (logs) del Sistema.

7) REGISTROS/ANEXOS