NORMATIVA

GESTIÓN DE CUENTAS Y PROCESOS DE AUTORIZACIÓN DE ACCESO

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.14	DOCUMENTO:	NORMATIVA DE GESTIÓN DE CUENTAS Y PROCESOS DE AUTORIZACIÓN DE ACCESO

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

Esta normativa tiene por objeto definir el protocolo y medidas de control para el acceso a cuentas, permisos de autorización y baja de usuarios, así como las normas de buen uso en los accesos a cuentas del personal del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

2) ALCANCE

Esta normativa será de aplicación para todo el personal del Ayuntamiento, incluyendo de la misma manera a aquellos usuarios que de forma puntual, y previa autorización al efecto, accedan a los servicios o sistemas del Ayuntamiento.

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

Recaerá en el Responsable del Sistema la asignación y autorización del alta y permisos, bloqueo y baja de usuarios, de manera consensuada con el Responsable de la entidad.

Cada responsable de área o departamento deberá informar al Responsable del Sistema de la baja de usuarios en su área/departamento, con el procedimiento que se designe en su caso, para que se proceda a la revocación del acceso por parte del Responsable del Sistema o la persona que este delegue.

4) DESARROLLO NORMATIVO

4.1) ALTA DE CUENTA Y CARACTERÍSTICAS

La creación de una cuenta con permisos de administrador, para operadores o desarrolladores deberá ser autorizada por el Administrador de Seguridad, o de la persona en quien delegue. Análogamente, para usuarios generales del Ayuntamiento, serán autorizados por el Responsable del Área/Departamento en el que desarrollen sus funciones.

En cualquier caso, la asignación de una cuenta se realizará comprobando previamente la identidad de la persona autorizada.

Una vez asignada la cuenta, la persona se convierte en su titular, debiendo velar, a partir de ese momento, por la seguridad de ésta, guardar secreto de sus credenciales de acceso y asumiendo toda su responsabilidad que se derive de su uso.

Toda cuenta de usuario deberá identificar, directa o indirectamente, al usuario y de forma unívoca.

No está permitido el uso de una cuenta de usuario por personas distintas a su titular, ni de cuentas asignadas a más de una persona o de carácter genérico (cuentas de invitado), salvo que sea estrictamente necesario por razones operacionales, esté autorizado por el Responsable del Sistema y esté documentado o se hayan implementado controles compensatorios para conocer la identidad de la persona que usa la cuenta en cada momento.

Una misma persona podrá ser titular de varias cuentas de usuario siempre que todas ellas estén debidamente identificadas.

4.2) BLOQUEO DE CUENTAS

Se procederá al bloqueo de las cuentas de usuario siempre que:

- Se tenga sospecha de estar siendo utilizada por otro individuo distinto a su titular.
- El titular esté haciendo uso de la misma incumpliendo la política de seguridad.
- Lo solicite el titular de la misma o su responsable directo.
- Se cumpla la fecha de caducidad establecida para la cuenta.

Para proceder al desbloqueo de una cuenta de usuario será necesario la solicitud del titular de la misma y la autorización del Responsable de Área/Departamento. Para cuentas de administración, operaciones y desarrolladores, deberá ser solicitada al Responsable del Sistema.

4.3) BAJA DE CUENTAS

Es responsabilidad del responsable del usuario que cause baja el solicitar la baja de la cuenta cuando el titular deje de necesitarla.

El departamento de personal deberá de notificar al Administrador de Seguridad la baja del usuario como trabajador en la administración de manera que no existan cuentas obsoletas o innecesarias.

El Administrador del Seguridad, aplicaciones o servicios deben revisar periódicamente las cuentas existentes y la correlación con los titulares de las mismas,. Para ello darán traslado de dicha relación de usuarios al Responsable del Área/Departamento correspondiente para su revisión y aprobación/eliminación de accesos.

4.4) AUTORIZACIÓN DE ACCESO

La responsabilidad de los accesos a cualquier sistema, aplicación, información o servicio o cualquiera de sus recursos recae en su responsable, el cual deberá revisar la lista de accesos concedidos al menos una vez cada 12 meses.

La concesión de acceso se llevará a cabo exclusivamente bajo el principio de “necesidad de uso” o de privilegios mínimos necesarios para su función.

4.5) USO Y RESPONSABILIDADES DE LOS USUARIOS

- Queda expresamente prohibido la divulgación de la clave o contraseña a otras personas, ya sean empleados o ajenas del Ayuntamiento.
- El usuario será el responsable de todas las actividades realizadas con su cuenta en los sistemas.
- No está permitido el uso de cuentas de usuario de otros titulares. Cuando por ausencias temporales (vacaciones, baja por enfermedad, permisos, etc.) se deban llevar a cabo tareas operativas a las que sólo tiene acceso esa cuenta, se asignarán los privilegios necesarios (previa solicitud y autorización) a la cuenta del personal que los sustituya en dichas tareas. Una vez el ausentado se reincorpore a su puesto, su responsable deberá solicitar la eliminación de los privilegios otorgados al sustituto.
- Se evitará teclear la contraseña si otras personas pudieran verla.
- No se anotarán nunca las contraseñas en lugares físicos o en formato electrónico sin protección, o accesibles por otras personas.
- Se cambiará la contraseña siempre que se tenga sospecha de que pueda haber sido comprometida, y siempre que el sistema o un administrador la haya asignado (manual o automáticamente).
- El usuario deberá informar al Departamento de Sistemas, de cualquier incidencia que detecte o sospeche de un uso inadecuado con su cuenta de usuario por los canales establecidos de notificación de incidencias.
- La información a la que se le ha concedido acceso deberá ser protegida por el usuario, en su uso (acceso, intercambio, transmisión por red, soportes, etc.) en base a la clasificación y normativas de seguridad establecidas para ésta
- En caso de inactividad del puesto de usuario, se bloqueará la pantalla y la sesión establecida.
- Cuando se asigne una nueva cuenta a un usuario, se le hará entrega de las responsabilidades y obligaciones con respecto a dicha cuenta y a sus credenciales.

4.6) MECANISMO DE AUTENTICACIÓN

Independientemente de si un sistema está en explotación o en producción, será necesaria la autenticación previa del usuario para poder acceder.

5) RESPONSABLE DEL CUMPLIMIENTO

El Responsable de Seguridad será el responsable de que se cumpla esta normativa en lo referente a gestión de cuentas y procesos de autorización

Si considerara que esta normativa es obsoleta o modificable, elevará propuesta al Comité de Seguridad para su modificación.

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.
- Política de Seguridad.

7) REGISTROS/ANEXOS