NORMATIVA

USO DE EQUIPOS REMOTOS Y EQUIPOS MÓVILES

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.22	DOCUMENTO:	NORMATIVA DE USO DE EQUIPOS REMOTOS Y EQUIPOS MÓVILES

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 regular las medidas de uso y control de los equipos remotos y/o portátiles del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

2) ALCANCE

Esta normativa aplica a todo el personal del Ayuntamiento y a todos los servicios con acceso a equipos remotos o equipos portátiles 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, a través del departamento de sistemas de la entidad, será el responsable de hacer cumplir y verificar que se cumplen las medidas de seguridad y uso descritas en esta normativa.

El Responsable de Seguridad estará capacitado para poder autorizar el uso por terceros de los equipos asignados a los usuarios del Ayuntamiento.

4) DESARROLLO NORMATIVO

El trabajo fuera de las instalaciones de la organización comprende tanto el teletrabajo habitual y permanente de los usuarios desplazados, como el trabajo ocasional, usando obligatoriamente, en ambos casos, activos municipales que serán entregados por el Departamento de Informática (Usualmente: ordenador portátil, tablet, teléfono móvil, etc.). Este modo de trabajo comprende también las conexiones remotas realizadas desde Congresos o sesiones de formación, alojamientos o, incluso, llamadas telefónicas de contenido profesional que sean realizadas o atendidas en áreas públicas.

El trabajo fuera de las instalaciones de la organización conlleva el riesgo de trabajar en lugares desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en sus instalaciones. Fuera de este perímetro de seguridad aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, lo que hace necesario adoptar medidas de seguridad adicionales.

Se incluyen seguidamente un conjunto de normas de obligado cumplimiento, que tienen como objetivo el reducir el riesgo cuando se trabaja fuera de las instalaciones del Ayuntamiento.

A. **Uso personal y profesional**. Los dispositivos móviles de computación y comunicación asignados a los usuarios del Ayuntamiento son para su uso exclusivo y solamente pueden ser utilizados para fines profesionales. No pueden prestarse a terceros.

B. **Necesidad de Autorización.** La salida fuera de las dependencias del Ayuntamiento de equipos y dispositivos informáticos precisa autorización previa del Responsanble de Sistemas.

C. **Uso de los canales de comunicación establecidos.** La transmisión de información y el acceso remoto se realizará únicamente a través de los canales establecidos, siguiendo los procedimientos y requisitos definidos para ello y adoptando las siguientes precauciones:
    a. Para identificarse se utilizará el certificado de empleado público que estará contenido en su tarjeta criptográfica. Las contraseñas a utilizar en la autenticación, estas deben ser robustas.
    b. Cerrar siempre la sesión al terminar el trabajo.
    c. Cifrar la información sensible, confidencial o protegida que vaya a ser transmitida a través de correo electrónico o cualquier otro canal que no proporcione la confidencialidad adecuada.

D. **Copias de seguridad.** Regularmente, debe realizarse copia de seguridad de la información contenida en los dispositivos móviles. Análogamente, es necesario adoptar las medidas adecuadas para la protección de dichas copias.
E. **Vigilancia permanente.** La documentación y los dispositivos móviles deben estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada en ellos o que pueda extraerse de ellos. En los desplazamientos en avión, este tipo de equipamiento no debe facturarse y deberá viajar siempre con el usuario.
F. Todos los equipos utilizados para administración y gestión de los servicios objeto de alcance del SGSI llevan **instalado y actualizado** un antivirus en el momento de ser entregados a su propietario. La actualización de la plantilla de antivirus está programada diariamente, es automática y desatendida.
G. **El acceso al sistema operativo** está protegido por contraseña. A través de una política de dominio, el sistema se bloquea a los 5 minutos de inactividad del mismo para así evitar el acceso no autorizado y debe ser desbloqueado introduciendo la contraseña del usuario.
H. **En caso de robo o pérdida** de un dispositivo móvil, el usuario debe interponer la denuncia oportuna ante las autoridades competentes y comunicarlo inmediatamente al Departamento de Sistemas. Se procederá a dar de baja el dispositivo y comunicar al proveedor de mantenimiento el nuevo estado, se actualiza el inventario indicando el estado de baja y se cierra el registro.
I. En relación con el **acceso remoto (vía web)**, deben adoptarse las siguientes cautelas:
    a. Los navegadores utilizados para el acceso vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
    b. Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
    c. Desactivar las características de recordar contraseñas en el navegador.
    d. Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
    e. Salvo autorización expresa, está prohibida la instalación de extensiones para el navegador.
J. **Está prohibido** manipular, abrir físicamente, liberar o desbloquear restricciones establecidas por la compañía cualquier dispositivo móvil proporcionados por el Ayuntamiento.
K. **Normativa interna.** Durante la actividad profesional fuera de las instalaciones del Ayuntamiento se seguirán las normas, procedimientos y recomendaciones internas existentes.

Comunicar cualquier incidente con la mayor rapidez que sea posible mediante el correo electrónico **informatica@baeza.net**

5) DISPOSITIVOS MÓVILES

5.1) AUTENTICACIÓN

Todos los dispositivos móviles corporativos que se cedan al personal contarán con un método de autenticación para evitar el acceso a la información contenida en el mismo por parte de personal no autorizado. Entre los métodos aceptados por la entidad para el desbloqueo del equipo una vez autentificado se encuentran los siguientes:

- Bloqueo por Pin.
- Bloqueo por huella dactilar.
- Bloqueo por reconocimiento facial.

5.2) SISTEMA ANTIVIRUS

El Ayuntamiento ha considerado que se requiere la instalación de un sistema antivirus en los dispositivos móviles de la organización que contengan o puedan contener información crítica (véase servicio de correo electrónico corporativo, o ficheros con documentación relevante). En el caso de sistemas operativos Android e iOS, se precisa la instalación de un antivirus.

5.3) INSTALACIÓN DE APLICACIONES

El Ayuntamiento actualmente no restringe la instalación de aplicaciones por parte del personal en los dispositivos móviles corporativos. Sin embargo, sólo deben instalarse aplicaciones desde las tiendas oficiales, y debe recordarse que estos dispositivos son solo para uso profesional.

6) RESPONSABLE DEL PROCEDIMIENTO

Será responsabilidad del Responsable de Seguridad velar por el cumplimiento de la presente normativa, previo consenso con el Responsable del Sistema de la información.

7) 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.

8) REGISTROS/ANEXOS