NORMATIVA

USO DE MEDIOS TECNOLÓGICOS

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.21	DOCUMENTO:	NORMATIVA DE USO DE MEDIOS TECNOLÓGICOS

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 medidas de uso y control de los medios tecnológicos utilizados en el 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 medios tecnológicos 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 de Sistemas de la Información, 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.

4) DESARROLLO NORMATIVO

4.1) PREMISAS

Esta regulación se basa en las siguientes premisas:

- Los medios tecnológicos son instrumentos que el Ayuntamiento pone a disposición de los empleados en el desempeño de sus funciones en el puesto de trabajo.
- Los medios tecnológicos están provistos por el Departamento de Sistemas.
- Se dispone de un inventario actualizado de los medios, siendo el Departamento de Sistemas el área encargada de gestionar dicho inventario.
- El Ayuntamiento posee el derecho legítimo a controlar el uso de los medios tecnológicos que pone a disposición de los empleados, salvaguardando el derecho a la intimidad del empleado, según establece la legislación vigente.

4.2) USO GENERAL DE LOS MEDIOS TECNOLÓGICOS

Para acceder a los medios tecnológicos es necesario tener asignada previamente una cuenta de usuario que establecerá el perfil necesario con el que se configuran las funciones y privilegios en las aplicaciones, según las competencias de cada usuario de acuerdo al “Procedimiento de Alta, Baja y Modificación de Cuentas de Usuario”.

Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta podrá ser desactivada en caso de una mala utilización.

Los usuarios tienen autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones.

Cuando un usuario deje de atender su equipo de trabajo durante un cierto tiempo, bloqueará la pantalla y su sesión, independientemente de que el equipo tenga configurado un bloqueo de pantalla automático, para evitar que alguna persona pueda hacer mal uso de sus credenciales, pudiendo llegar a suplantarlo.

En general, se prohíbe el uso de los medios tecnológicos por cualquier empleado cuando:

- Se viole la legislación vigente (leyes de protección de datos, de licencias de programas, derechos de autor, etc.). La información contenida en los Sistemas de Información de Ayuntamiento es de su propiedad, por lo que queda prohibido comunicar, divulgar, distribuir o poner en conocimiento o alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa.

- Se realice con fines privados con ánimo de lucro.
- Pueda dañar la reputación y buen nombre del Ayuntamiento.
- Se atente contra la seguridad o eficiencia del Ayuntamiento.

4.3) USO EFICIENTE DE LOS MEDIOS TECNOLÓGICOS

Dentro de las medidas de austeridad y reducción del gasto del Ayuntamiento se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios:

- Apagar el PC al finalizar la jornada laboral.
- Los recursos de almacenamiento de red son compartidos y limitados, por lo que se hará un uso responsable de los mismos y se almacenará únicamente aquella información que sea estrictamente necesaria y relacionada con el ámbito laboral.

4.4) USO DEL CORREO ELECTRÓNICO

El Ayuntamiento pone a disposición de sus empleados una cuenta de correo electrónico con el fin de poder comunicarse e intercambiar información en el desarrollo de sus funciones.

Se tendrán en cuenta las directrices dictadas en la norma de Clasificación de Información y la norma de Intercambio de Información para el envío de información en función de su nivel de clasificación.

A continuación, se incluye un conjunto de normas que tienen como objetivo reducir el riesgo en el uso del correo electrónico:

- Utilizar el correo electrónico exclusivamente para propósitos profesionales. Gran parte de los mensajes de correo electrónico no deseados que llegan a la entidad tienen su origen en un uso no profesional de las cuentas de correo. Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de ataque.

  No debe de utilizarse la dirección de correo electrónico de la entidad para registrarse en páginas web de uso personal.

- No ceder el uso de las cuentas de correo. Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales - para los que deberá solicitarse y obtenerse la correspondiente autorización -, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial.

  Además de ello, es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios.

- Revisar la barra de direcciones antes de enviar un mensaje. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo “Con Copia (CC)”. Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.
- No se permitirá suplantar la identidad de otro usuario.
- No se deben enviar o reenviar correos de forma masiva. Si se envía por necesidad un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO o BCC), evitando su visibilidad a todos los receptores del mensaje.
- No enviar mensajes en cadena. Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe notificar la incidencia.
- No responder a mensajes de Spam. La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envían a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa al Ayuntamiento. En cualquier caso, nunca debe responderse a los mismos.

- Utilizar mecanismos de cifrado de la información. Los mensajes que contengan información sensible, confidencial o protegida deben cifrarse. El Departamento de Sistemas pondrá a disposición de los usuarios que lo precisen el acceso a la aplicación necesaria para el cifrado de información.
- Asegurar la identidad del remitente antes de abrir un mensaje. Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) del usuario atacado. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información sensible, confidencial o protegida a petición de un correo del que no se puede asegurar la identidad del remitente debe rechazarse.

  Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).

- Desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos.
- Limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.
- Utilizar herramientas de análisis contra código dañino. La utilización de herramientas tales como antivirus y cortafuegos ayuda a detectar el código malicioso y a mitigar sus efectos. Por ello, debe configurarse el antivirus con la opción de analizar el correo electrónico entrante.
- No abrir correos basura ni correos sospechosos. Aun cuando un mensaje no deseado hubiera traspasado el filtro contra spam, no debe abrirse, debiendo reportarse el correspondiente incidente de seguridad. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.
- No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso.

  Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).

- Informar de correos con virus, sin reenviarlos. Si el usuario detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente de seguridad y no reenviarlo, para evitar su posible propagación.
- No utilizar el correo electrónico como espacio de almacenamiento. La capacidad de espacio en los servidores de correo del Ayuntamiento es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes o que se realice un borrado, más o menos selectivo, de los mensajes almacenados. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieren quedado obsoletos.
- En relación con el acceso remoto (vía web) al correo electrónico, deben adoptarse las siguientes cautelas:
    - Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
    - 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.
    - Desactivar las características de recordar contraseñas para el navegador.
    - 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.
    - Salvo autorización expresa, está prohibida la instalación de extensiones para el navegador.
    - Además de lo anterior, cualquier información sensible, confidencial o protegida que permanezca almacenada en el servidor de correo podría ser accedida por un atacante, lo que aconseja su borrado.

4.4.1) ADVERTENCIAS LEGALES

En todas las comunicaciones por correo electrónico que realice el Ayuntamiento hacia el exterior se incluirá al final del texto:

Este mensaje está dirigido únicamente a su destinatario y puede contener información CONFIDENCIAL o PRIVILEGIADA sometida a secreto profesional y/o cuya divulgación está prohibida por la legislación vigente. Si ha recibido este mensaje por error, debe saber que su lectura, copia y uso no están autorizados. Le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción, así como la de cualquier documento adjunto.

El correo electrónico vía Internet no permite asegurar la confidencialidad de los mensajes que se transmiten ni su integridad o correcta recepción. El Ayuntamiento no asume responsabilidad por estas circunstancias y se reserva el derecho a ejercer las acciones legales que le correspondan contra todo tercero que acceda de forma ilegítima al contenido de este mensaje y al de los ficheros contenidos en el mismo.

El Ayuntamiento cumple con la legislación en materia de protección de datos de carácter personal. De acuerdo a lo establecido en el Reglamento General de Protección de Datos, el Reglamento (UE) 2016/679 y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, le informamos que el Ayuntamiento dispone de su correo electrónico de manera lícita, y es responsable de los datos personales que puedan contenerse en este email. Este mensaje ha sido enviado conforme a los datos que existen en nuestros ficheros informatizados.

El Ayuntamiento cuenta con las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos que maneja, cumpliendo los requisitos básicos exigidos en el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010 de 8 de enero.

Según los derechos que le amparan, podrá retirar sus consentimientos en cualquier momento, así como oponerse al tratamiento, limitar el mismo, acceder, rectificar, suprimir los datos y/o ejercer su derecho a portabilidad, enviando su solicitud a través del correo electrónico sac@baeza.net o en la dirección postal Pje. Cardenal Benavides, 10, 23440 Baeza, Jaén, España. Igualmente podrá presentar una reclamación ante el Consejo de Transparencia y Protección de Datos de Andalucía si detecta alguna irregularidad en la recogida y/o tratamiento de sus datos personales.

4.5) USO DE INTERNET

El Ayuntamiento pone a disposición de sus empleados conexión a Internet para facilitar el desarrollo de sus funciones:

- Se entiende “uso de internet”, cualquier acceso a páginas web, grupos de noticias (News), Chat, IRC, telnet, ftp, videoconferencias, con destino externo a la red del Ayuntamiento.
- Se establecerán registros automáticos de las personas y procesos que usen Internet, quedando registrados los sitios concretos a los que accede.
- Los usuarios son los únicos responsables de todas las actividades realizadas.

4.5.1) USO ACEPTABLE

Se podrá usar Internet para:

- Acceso a cualquier tipo de información relacionada con el desempeño de las funciones del empleado.
- Acceso a información con fines particulares solamente de forma puntual y no abusiva.

4.5.2) USO NO ACEPTABLE

Queda prohibido el uso de Internet en los siguientes términos:

- Para suplantar la identidad de un usuario.
- Con fines particulares y en horario laboral, salvo usos puntuales y no abusivos.
- Juegos de entretenimiento, juegos de azar, concursos, subastas, etc.
- Descarga de software ilegal.
- Cuando no estén estrictamente relacionadas con las funciones del trabajador, las siguientes actividades:
    - Descarga de cualquier tipo de software sin autorización del Responsable de Seguridad.
    - Acceso a servicios como chat, IRC, telnet, ftp, videoconferencias.
- En ningún caso, uso de programas “peer-to-peer” para compartir archivos.

- Descargas continuadas de cualquier tipo de archivos o de volúmenes de información muy grandes que puedan degradar la conexión a Internet y por tanto afectar al resto de los empleados.

4.6) ESTACIONES DE TRABAJO Y PERIFÉRICOS

A cada nuevo usuario que se incorpore a la Entidad y así lo precise, el Departamento de Sistemas le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales.

4.6.1) USO ACEPTABLE

Se permite el uso de PCs o estaciones de trabajo para:

- Realización de trabajos y actividades relacionadas con el desempeño de las funciones del empleado.
- Guardar información propiedad del usuario, relacionada con el desempeño de sus funciones. Esta carpeta deberá estar permanentemente autorizada a ser revisada por el antivirus corporativo. La información contenida en ella es responsabilidad del trabajador.
- El usuario debe participar en el cuidado y mantenimiento del equipo asignado, detectando la ausencia de cables y accesorios, dando cuenta al Departamento de Sistemas de tales circunstancias.

4.6.2) USO NO ACEPTABLE

No está permitido el uso de estaciones de trabajo o PC para lo siguiente:

- Realizar trabajos particulares, o con fines privados, durante el horario laboral.
- Modificación de la configuración física hardware de las estaciones sin autorización.
- Instalación de software libre no autorizado o de software no licenciado por el Ayuntamiento. La instalación autorizada de software siempre debe hacerse bajo la supervisión del Departamento de Sistemas.
- Instalación de cualquier paquete software que pueda causar un mal funcionamiento o degradación en la red o en los servicios del Ayuntamiento.
- Cambio en la configuración de las estaciones, excepto en aquellos valores que atañen directamente a la operatividad: configuración de pantalla, escritorio, valores de usuario, aplicaciones, etc. No está en ningún caso permitido cambiar la configuración de la red, así como el antivirus, cortafuego personal o cualquier otro control de seguridad.
- Instalación y uso de software orientado a conseguir privilegios en la red o realización de ataques a otros equipos (generadores de tráfico, escáneres de puertos, escuchas de tráficos, etc.)
- Guardar información como aplicaciones, ejecutables, etc. que sea ilegal o susceptible de contener software malicioso.
- Hacer uso de cualquier tipo de juego.

Así mismo, sobre periféricos no está permitido:

- El uso abusivo del teléfono (fijo o móvil) para realizar llamadas particulares, entendiendo por abusivo la reiteración en valores altos en coste o duración de llamadas.
- El uso de las impresoras, escáneres, plotters, y demás periféricos para fines particulares dentro del horario laboral, o fuera de éste, de forma indiscriminada o sin autorización expresa.

5) RESPONSABLE DEL CUMPLIMIENTO

El Responsable de Seguridad será la persona indicada para verificar que se se está cumpliendo en todos los Servicios/Áreas/Departamentos y estaciones de trabajo las medidas descritas 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 Clasificación de Información.
- Normativa de Intercambio de Información.
- Procedimiento de Alta, Baja y Modificación de Cuentas de Usuario.

7) REGISTROS/ANEXOS