NORMATIVA

INTERCAMBIO DE INFORMACIÓN

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.03	DOCUMENTO:	NORMATIVA DE INTERCAMBIO DE INFORMACIÓN

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 establecer la metodología de intercambio de información del Excmo Ayuntamiento de Baeza, (en adelante, Ayuntamiento), tanto si se trata de intercambios entre departamentos, con las AAPP o con terceros y las normas a cumplir por el personal de la entidad.

2) ALCANCE

El alcance de la presente normativa abarca a todos los departamentos o áreas del Ayuntamiento, así como a todo el personal usuario que intervengan en el proceso, sea externo o interno para intercambio con terceros, salvo para relaciones entre departamentos y con otras administraciones públicas, en ese caso, se deberá de utilizar la herramienta de gestor de expedientes propia del Ayuntamiento de Baeza entre departamentos y el SIR que es la infraestructura básica que permite el intercambio de asientos electrónicos de registro para las AAPP, de forma segura y con conformidad legal, independientemente de la aplicación de registro utilizada, para dejar constancia del intercambio de información.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de Seguridad, Responsable del Sistema, Responsables de los Servicios 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

Será responsabilidad del Responsable del Sistema implementar todas las medidas de seguridad encaminadas a la seguridad de los procesos de intercambio de información, o en su defecto, la persona que este delegue.

4) DESARROLLO NORMATIVO

4.1) NORMAS PARA EL INTERCAMBIO DE INFORMACIÓN

4.1.1) NORMAS DIRIGIDAS A TODOS LOS USUARIOS

- Los empleados deben velar por el cumplimiento de los Acuerdos de Intercambio con los proveedores de servicios.
- Los empleados tienen la obligación de ponerse en contacto con su responsable en caso de observar que alguna parte no cumple los Acuerdos de Intercambio con los proveedores de servicios.

4.1.2) NORMAS DIRIGIDAS A LA DIRECCIÓN JURÍDICA

- La Dirección Jurídica debe establecer los requerimientos legales para el intercambio de información con terceras partes.
- De igual manera, debe revisar o crear un acuerdo de intercambio de información en los contratos con los terceros a los que se les deba entregar o enviar información específica.

4.1.3) NORMAS DIRIGIDAS A LOS RESPONSABLES DE DEPARTAMENTOS

- El intercambio de información de la organización con sus proveedores de servicios debe ser efectuado una vez se hayan establecido los correspondientes Acuerdos de Intercambio y nunca antes de haberse establecido los mismos.
- Los proveedores de servicios con los cuales haya intercambio información de la organización deben acogerse a las políticas de seguridad de la información y deben regirse por los Acuerdos de Intercambio establecidos.

4.1.4) NORMAS DIRIGIDAS A LOS SERVICIOS GENERALES

- Se han definido los siguientes procedimientos para el intercambio, transmisión y transporte de medios de almacenamiento y documentos a fin de proteger la información sensible contra divulgación o modificaciones, ya sea este intercambio interno o externo.

- Los servicios de mensajería usados para el intercambio de medios que puedan contener información sensible serán confiables. Esto significa que se realizará siempre con las empresas con las que se tiene acuerdo específico de intercambio de información y seguros asociados.
- Los envíos que puedan contener información sensible se realizarán siempre con un remitente y un receptor físicos claramente definidos, nunca se enviarán a nombre de un departamento.
- Los medios que puedan contener información sensible y vayan a ser enviados, estarán siempre vigilados y se almacenarán de forma segura hasta su intercambio.
- El envío de medios que puedan contener información sensible no se realizará nunca por correo ordinario u otro medio no seguro.
- La información clasificada como de USO INTERNO puede circular libremente dentro las instalaciones del Ayuntamiento. Su circulación fuera de él será sólo para personal autorizado.
- Para la información clasificada como de CONFIDENCIAL o SECRETO, existirá un listado las personas autorizadas a acceder a la misma. Las copias que se realicen de este tipo de información deberán estar expresamente autorizadas por el responsable de la misma y de la conformidad del Responsable de Seguridad.

Se han definido las siguientes medidas para proteger las conversaciones telefónicas de interceptaciones, escuchas malintencionadas, redifusiones, etc.

- Se evitará en medida de lo posible tratar durante una llamada telefónica temas confidenciales o de carácter personal ya que es un medio poco seguro.
- Si fuera imprescindible tratar de un tema confidencial por teléfono, se realizará en un lugar aislado, nunca en una zona común de trabajo, se comprobará en medida de lo posible que no hay personas atentas o que puedan escuchar por error parte de la conversación.

4.1.5) NORMAS DIRIGIDAS AL DEPARTAMENTO DE SISTEMAS

El Departamento de Informática dictará las siguientes directrices para asegurar todos los intercambios de información dependiendo de su medio.

Cuando se trata de un medio físico las normas son:

- Medios Removibles (HDs, USBs, etc). Todos los medios removibles que pudieran contener información sensible serán cifrados, y la contraseña del cifrado será enviada por medio alternativo al receptor del mensaje tal y como se describe en el procedimiento de envío seguro de contraseñas, nunca lo contendrá el mismo paquete que contenga el medio. Para gestionar estos medios, se seguirán las directrices para convertir el medio seguro tal y como se detalla en el documento “NR.22.Uso de Equipos Remotos y Equipos Portátiles”.

Para medios lógicos:

- Correo Electrónico. Todos los correos en el Ayuntamiento deberían ser enviados siguiendo las normas descritas en el documento “NR.21.Uso de Medios Tecnológicos.docx”.
- Transferencia de archivos por FTP/FTPS. Todos los envíos usando FTP, en caso de contener información sensible o confidencial, se realizará usando el protocolo seguro de envío FTPS en lugar del no seguro FTP. Las credenciales se enviarán siguiendo el método seguro de envío de contraseñas.
- Transferencia de archivos por HTTP/HTTPS. Todo sitio web publicado en el Ayuntamiento que pueda contener información confidencial o sensible se publicará usando el protocolo seguro HTTPS en lugar del no seguro HTTP. Las credenciales se enviarán siguiendo el método seguro de envío de contraseñas.

5) ACUERDOS DE INTERCAMBIO DE INFORMACIÓN

A continuación, se describen las normas de comunicación bidireccional entre el Ayuntamiento y la ciudadanía:

- Se utilizará la sede electrónica municipal para el intercambio de información siempre.
- En el caso que no sea posible utilizar la sede electrónica por limitaciones técnicas imputables al tercero, habría que estudiar por el responsable de sistemas su idoneidad de usar el correo electrónico o teléfono como canal de comunicación como último recurso y con las garantías descritas en esta norma.
- Se incluirá el criterio elegido para la clasificación de la información. Si las terceras partes no tienen inconveniente se usará la clasificación adoptada por el Ayuntamiento, descrita en el documento “NR.02.Clasificación de la Información.docx”.

- El acuerdo incluirá quién tendrá acceso a la información, así como las categorías de información que pueden ser compartidas por los diferentes medios disponibles.
- Toda la información necesaria para la gestión y prestación del servicio llevado a cabo por la institución debe estar accesible para las personas autorizadas y documentada de forma completa.
- En el acuerdo se establecerán los controles de acceso necesarios para mantener la confidencialidad e integridad de la información.
- Se especificarán las partes responsables de la cadena de custodia en cada una de las etapas del proceso de intercambio de información.

Las normas anteriores permiten organizar y realizar el seguimiento del servicio prestado a la ciudadanía.

Estas normas son las que se deben cumplir siempre, aún en el caso de contar con una situación no prevista en la metodología general y que necesite de actividades nuevas para resolverla.

6) MENSAJERÍA ELECTRÓNICA

El uso del correo electrónico genera importantes amenazas al sistema de información. Infección de equipos por malware, envíos de información sin las medidas de seguridad correctas o sustracción de información son algunas de las amenazas que pueden afectar a los equipos y usuarios.

En este apartado se detallan las medidas y controles que se implementan en las instalaciones del Ayuntamiento para asegurar la información que se intercambia a través de los sistemas de mensajería electrónica.

6.1) PROCEDIMIENTO

Para asegurar un correcto tratamiento de la seguridad en la mensajería electrónica se definen los siguientes controles que aplican a los sistemas y usuarios de los sistemas de correo electrónico:

- Normas de seguridad aplicables a usuarios. Detalladas en el documento “NR.24.Contratación y Relaciones con Terceros.docx “.
- Protección contra códigos maliciosos, SPAM, etc. Definidos en el documento “PR.20.Prevención y Control contra Código dañino”.
- Protección de los servidores de correo del Ayuntamiento:
    - Los equipos son actualizados periódicamente como parte del procedimiento de actualización de software definido en el documento “PR.06.Gestión de cambios y versiones”.
    - Se controla el acceso a dichos servidores solo a personal autorizado tal y como se especifica en el documento “NR.05.Seguridad Física y de acceso al CPD.docx”.
    - Se monitoriza el acceso y utilización de los servidores de correo y las operaciones realizadas en los mismos por los diferentes tipos de usuarios, llevándose a cabo un registro de auditoría y reporte de los mismos siguiendo los controles y medidas detallados en el documento “NR.19.Auditorías y Registro de los Sistemas”.
    - Se realizan copias de seguridad de los servidores de correo siguiendo las medidas y controles detallados en la política “NR.11.Copias de Seguridad (Backup)”.
- Protección del acceso por parte de los usuarios a los buzones de correo:
    - El acceso está controlado mediante la combinación de usuario y contraseña. Está definida una política de contraseñas segura como se indica en el documento “ENS.CON.Política de contraseñas”.
    - El acceso mediante el webmail, el método más utilizado desde fuera de la oficina, se realiza de forma segura por HTTPS.
    - Las sesiones webmail son finalizadas tras el paso de un tiempo de inactividad.
    - Se ha definido una política escritorio y pantalla limpios que ayuden a minimizar la posibilidad de fugas de información como se recoge en los documentos de “NR.08.Seguridad de la Red, Servicios de Red y Perímetro” y “PR.02. Seguridad física y ambiental”.
    - Se ha definido una política de equipos desatendidos como se recoge en el documento “NR.06.Seguridad Física del Equipamiento”.
- Se tomarán las siguientes medidas para el envío de información por correo electrónico:
    - El asunto de los mensajes debe ser poco descriptivo si contienen información privilegiada.
    - El nombre de los ficheros que se ajusten en comunicaciones que contengan información confidencial debe ser poco significativo.

- Los mensajes se enviarán firmados digitalmente y cifrados cuando su clasificación así lo requiera. Se utilizará sistemas de clave pública/privada (PGP, GPG, PKI) en vez de sistemas de cifrado simétrico, y éste sólo se usará en aquellos casos en los que el receptor no pueda leer mensajes cifrados con clave asimétrica.
- Antes de enviar un mensaje con información confidencial los usuarios deben revisar y comprobar la validez de los destinatarios que van a recibir dicha información. Si existe un acuerdo de intercambio de información se comprobará que el destinatario está incluido dentro de la lista de direcciones de correo seguras de dicho acuerdo.
- Los usuarios no deben reenviar mensajes con información confidencial fuera del ámbito de comunicación de la misma.

7) ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN

El Ayuntamiento establece diferentes tipos de acuerdos de confidencialidad dependiendo de la relación que la persona que debe firmarlo tiene con la compañía y el rol que desempeña.

Todos estos acuerdos de confidencialidad están de acuerdo con las legislaciones y normativas aplicables.

Todos estos acuerdos de confidencialidad deben ser firmados obligatoriamente tal y como lo establece la política de seguridad del Ayuntamiento según las circunstancias en las que aplique cada uno tal y como se detalla a continuación.

Acuerdo de Confidencialidad General

Acuerdo de Confidencialidad que deben firmar y aceptar todos los empleados del Ayuntamiento con independencia del puesto que vayan a desempeñar. En este acuerdo se establecen cláusulas de:

- **Confidencialidad:** Aplica a la información relacionada con los programas, información de carácter confidencial, procedimientos de desarrollo e implantación, el know-how, la estructura organizacional... Aplica durante tiempo indefinido.
- **No concurrencia:** Establece la imposibilidad de desarrollar o colaborar en el desarrollo directa o indirectamente de cualquier producto o tecnología similar a los productos del Ayuntamiento. Aplica durante la relación con el Ayuntamiento.
- **No posesión:** Establece la prohibición de tener en su poder copia alguna de código fuente de los programas a los que tenga acceso. Aplica durante tiempo indefinido.
- **Propiedad intelectual:** Se establece que el Ayuntamiento es el único titular de los derechos de sus productos.
- **Incumplimiento y responsabilidades**: Se establecen las responsabilidades derivadas del incumplimiento de dichas cláusulas.

Acuerdo de Confidencialidad

Acuerdo de Confidencialidad que deben firmar y aceptar todos los empleados que dan soporte a los servicios objeto de alcance del SGSI, dada la posibilidad existente de acceso a información confidencial de la ciudadanía que forma parte de dichos servicios. En este acuerdo se establecen cláusulas de:

- **Confidencialidad:** Aplica a toda aquella información de las personas implicadas del Ayuntamiento que se utilice en el desempeño de sus funciones para la prestación de los servicios relativos a la gestión y al soporte técnico. Aplica durante tiempo indefinido.
- **No posesión:** Establece la prohibición de tener en su poder copia alguna en papel o soporte electrónico de información perteneciente a los ciudadanos contenida en la plataforma relativa. Aplica ante tiempo indefinido.
- **Tratamiento de Datos:** Gestión confidencial y diligente de la documentación confidencial necesaria para la prestación de los servicios.
- **Incumplimiento y responsabilidades:** Se establecen las responsabilidades derivadas del incumplimiento de dichas cláusulas.

Acuerdo de Confidencialidad Desvinculación

Acuerdo de Confidencialidad que deben firmar y aceptar todos los empleados que abandonan la entidad y que han prestado servicio o desempeñado funciones con acceso a información contenida en los sistemas. En este acuerdo se establecen cláusulas de:

- **Confidencialidad:** Aplica a toda aquella información de las personas implicadas del Ayuntamiento que se utilice en el desempeño de sus funciones para la prestación de los servicios relativos a la gestión y al soporte técnico. Aplica durante tiempo indefinido.
- **No posesión:** Establece la prohibición de tener en su poder copia alguna en papel o soporte electrónico de información perteneciente a la ciudadanía. Aplica ante tiempo indefinido.
- **Incumplimiento y responsabilidades:** Se establecen las responsabilidades derivadas del incumplimiento de dichas cláusulas.

Acuerdo de Confidencialidad con terceros

Acuerdo de Confidencialidad que deben firmar y aceptar los terceros que tengan o puedan llegar a tener acceso a información considerada como confidencial por el Ayuntamiento. Si los contratos de los proveedores incluyen una cláusula de confidencialidad que cubra las necesidades del Ayuntamiento, dicha cláusula es aceptada como válida sin necesidad de firmar un acuerdo de confidencialidad específico proporcionado por el Ayuntamiento.

El acuerdo de Confidencialidad deberá incluir:

- Definición de información confidencial y exclusiones.
- Obligaciones respecto de la información confidencial.
- Propiedad intelectual y Protección de Datos.
- Responsabilidad y Garantías.
- Incumplimiento.
- Duración del acuerdo.

8) RESPONSABLE DEL CUMPLIMIENTO

La responsabilidad final de la presente normativa y del proceso de intercambio de documentación recae sobre el Responsable de Seguridad.

9) 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 Interna/Procedimientos:

- NR.02.Clasificación de la Información
- ENS.CRV.Política de Copias de Seguridad, Restauración y Verificación
- NR.06.Seguridad Física del Equipamiento
- NR.08.Seguridad de la Red, Servicios de Red y Perímetro
- NR.21.Uso de Medios Tecnológicos
- NR.22.Uso de Equipos Remotos y Equipos Portátiles
- NR.05.Seguridad Física y de acceso al CPD
- NR.19.Auditorías y Registro de los Sistemas
- NR.24.Contratación y Relaciones con Terceros
- PR.02. Seguridad física y ambiental
- PR.06.Gestión de cambios y versiones
- PR.20.Prevención y Control contra Código dañino

10) REGISTROS/ANEXOS

- Contrato de encargado de tratamiento con acceso a datos.
- Acuerdos de Confidencialidad de los trabajadores del Ayuntamiento.

ANEXO 1: TABLA RESUMEN AL TRATAMIENTO DE LA INFORMACIÓN

TRATAMIENTO DE LA INFORMACIÓN. CONCEPTOS	Confidencial ---------- Datos Personales Categoría especial	Confidencial ---------- Datos Personales no incluidos en los artículos 8 a 10 del RGPD.	Uso Interno	Pública
Transmisión por Redes Inalámbricas	Cifrado Fuerte	Cifrado Fuerte	Cifrado	
Transmisión por Red Interna	Cifrado			
Transmisión por Red Externa con Conexión Directa	Cifrado	Cifrado		
Transmisión por Red Pública	Cifrado	Cifrado		
Transmisión por Correo, FTP, etc. en Red Interna	Cifrado			
Transmisión por Correo, FTP, etc. en Red no Interna	Cifrado	Cifrado		
Identidad del remitente en correo electrónico	Exigir			
Borrado sin posibilidad de recuperación	Exigir	Exigir		
Cifrado en Soporte fuera de dependencias del Ayuntamiento	Cifrado	Cifrado		
Cifrado Soportes dentro de dependencias, cuando no tengan protecciones adecuadas	Cifrado	Cifrado		
Transmisión por fax. (Siempre eliminar copias de memoria)	Evitarse o Ponerse en contacto con Receptor	Evitarse o Ponerse en contacto con Receptor	Evitarse o Ponerse en contacto con Receptor	
Necesaria autorización para sacar soporte fuera de dependencias del Ayuntamiento	SI	SI	SI	

Devolución de información por terceros y borrado de copias	Exigir	Exigir	Exigir	
Tratamiento por personal externo	SI, con acuerdo confidenc. Autorización expresa para datos personales	SI, con acuerdo confidenc. Autorización expresa para datos personales	SI, con acuerdo confidenc.	SI
Tratamiento solo por personal autorizado	SI	SI		
Tratamiento solo por personal autorizado expresamente	Exigir	Exigir si son Datos Personales		
Autorización necesaria para hacer copias	Responsable de la Información Responsable del Servicio si contiene datos de carácter personal	Por el Responsable del Servicio si son datos personales	NO	NO