NORMATIVA

CLASIFICACIÓN DE LA INFORMACIÓN

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.02	DOCUMENTO:	NORMATIVA DE CLASIFICACIÓN DE LA 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

El objeto del presente documento es el de establecer los criterios de clasificación de la información del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

En esta normativa se detallará, igualmente, los métodos de destrucción de la información en base a la clasificación con la que anteriormente haya sido etiquetada.

2) ALCANCE

Esta normativa aplica a todos los departamentos del Ayuntamiento, y es de obligado cumplimiento por parte de todos los intervinientes en este proceso.

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

- La responsabilidad de establecer la clasificación de una determinada información es del responsable de la entidad, previa consulta con el responsable de cada uno de los departamentos, áreas o servicios del Ayuntamiento.
- La responsabilidad de establecer el etiquetado la información, con la aprobación del Responsable de Seguridad, es de quien la genera o modifica.
- La responsabilidad de establecer el etiquetado de clasificación del activo, con la aprobación del Responsable, es del Gestor del activo.
- El usuario, como persona que accede a la información clasificada asume las siguientes responsabilidades:
    - Proteger adecuadamente la información a su cargo.
    - Mantener la debida reserva ante terceros sobre su condición de titular.
    - Cooperar con el Responsable de Seguridad en todo aquello que se relacione con la seguridad la información CONFIDENCIAL o de USO INTERNO en su puesto de trabajo, en su entorno laboral y en toda actividad que intervenga.

4) DESARROLLO NORMATIVO

4.1) REVELACIÓN O DISTRIBUCIÓN

La información almacenada o tratada se clasifica, de acuerdo con el criterio de utilización y revelación o distribución en:

Pública o publicable (0)	Información de uso general y público
Uso interno (1)	Información para uso interno de Ayuntamiento. La revelación de esta información supone un riesgo para la entidad.
Confidencial (2)	Información confidencial cuya revelación no autorizada podría causar daño a la entidad
Secreta (3)	Información confidencial cuya revelación no autorizada causaría un daño considerable a la entidad

Pública o publicable:

- Información pública del Ayuntamiento sobre las características de las actividades prestadas.
- Información de catálogo de procedimientos y servicios del Ayuntamiento.

Uso interno:

- Información relativa a documentación específica del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) del Ayuntamiento con alcance en el mismo de las actividades prestadas.
- Información relativa a la Configuración de los Sistemas de Información del Ayuntamiento.

Confidencial:

- Información relativa a Incidencias de soporte fruto de la explotación de procedimientos y servicios.
- Información de la configuración y administración de la arquitectura del sistema y comunicaciones a fin de adecuar los recursos a las necesidades de la ciudadanía, maximizar la capacidad de producción y minimizar los riesgos de explotación.
- Actas de Aprobación del SGSI.

Secreta:

- Información de cuentas de ciudadanía de servicios e Información de cuentas de Administración del Sistema y de las aplicaciones.

4.2) IMPACTO

De acuerdo al impacto en la entidad:

- Si la información no está disponible supondrá:
    - Ralentización de la Administración.

Secreta: La no disponibilidad de información relativa a información de la ciudadanía y cuentas de administración del Sistema y de las aplicaciones.

- Impacto en la ciudadanía.

Confidencial: Si la información relativa a configuraciones del Sistema o incidencias en soporte de servicios no está disponible, podrá provocar un impacto elevado en clientes.

- Afecta al trabajo diario de empleados.

Uso interno: Si la información relativa a configuraciones de componentes software del Sistema, documentos de SGSI o información del catálogo de servicios y procedimientos no está disponible, dicho hecho podrá afectar al trabajo de empleados del Ayuntamiento e incluso a la propia ciudadanía.

- Ninguna de las anteriores.

Pública o publicable: Si la información pública del Ayuntamiento sobre las características del Sistema no está disponible en la página, dicho hecho no repercute u ocasiona impacto elevado para el mismo.

4.3) REQUERIMIENTOS LEGALES

De acuerdo con los requerimientos legales asociados a dicha información, la clasificación es la siguiente:

- **Criterio: Obligatoriedad de entregar la información en un plazo acordado.**
    - La información es obligatoria por ley. (Secreta)
    - La información es obligatoria por contrato. (Confidencial)
    - La información es obligatoria por política interna del Ayuntamiento. (Uso interno)
    - No existe obligación regulatoria o normativa. (Pública o publicable)
- **Criterio: Obligatoriedad de mantener íntegra la información.**
    - Obligatorio por ley. (Secreta)
    - Obligatorio por contrato. (Confidencial)
    - Obligatorio por política interna del Ayuntamiento. (Uso interno)

- No existe obligación regulatoria o normativa. (Pública o publicable)

4.4) GENERACIÓN DE FRAUDE

De acuerdo con la potencial generación de fraude, la información se clasifica en:

- Modificación no autorizada puede producir o generar fraude (Secreta).
- Modificación no autorizada no puede producir o generar fraude (Pública o publicable, Uso interno, Confidencial).

4.5) CRITICIDAD O VALOR DE LA INFORMACIÓN

De acuerdo con la criticidad de los activos o porcentaje de activos que se verían expuestos a una amenaza, la clasificación es la siguiente:

Criticidad alta (Secreta)	● Se ven expuestos los datos de la ciudadanía.. ● Se ven expuestos datos que posibilitan fraude o pueden suponer pérdidas importantes para la entidad. ● Los activos expuestos son activos financieros o en general, información secreta. ● Los Sistemas que se ven expuestos soportan actividades y procedimientos críticos (por ejemplo. Procesos de gestión, sistemas de red, sistemas de facturación, etc.). ● Se ven expuestos todos los datos.
Criticidad media (Uso interno, Confidencial)	● Los activos expuestos contienen información confidencial. ● Los Sistemas que se ven expuestos soportan procesos internos necesarios para el funcionamiento de la entidad. ● Solo se ven expuestos partes de los datos.
Criticidad baja (Público o publicable)	● Los activos expuestos no son datos sensibles. ● Las plataformas no soportan procesos críticos.

4.6) MECANISMOS DE ACCESO

- Información accedida a través de XXXX. Si se trata de información personal y de perfiles del sistema o plataforma, dicha información se clasifica según el mecanismo de acceso en:
  - (Secreta).
  - Información accedida a través del sistema. (Secreta).
  - Información accedida a través de Gestión de identidades de usuario. (-)
  - Otras.

De acuerdo con el acceso a la información, esta puede ser accedida por usuarios finales, administradores, operadores:

- De forma Web (A través de un frontal). (Secreta)
- A través de aplicaciones específicas. (Secreta)

4.7) VALORACIÓN ÁCIDA

Con el objeto de identificar los requisitos de seguridad de cada uno de los activos, se les asigna una valoración de 1 a 5, en 5 características de seguridad.

Las características valoradas son las siguientes:

- Autenticación.
- Confidencialidad.
- Integridad.

- Disponibilidad.
- Auditabilidad o Trazabilidad.

Cuanto mayor sea la valoración de un activo en un requisito, más importante es el mantenimiento de ese requisito para la entidad y más impacto causa la degradación de ese requisito.

4.8) PRIVACIDAD

Según el tipo de datos o información que contenga un documento, deberá especificarse de qué tipo se trata:

- NO IP: No contiene datos de carácter personal.
- IP A: Contiene datos de carácter personal tales como nombre, apellidos, dirección, etc.
- IP B: Contiene datos de carácter financiero.
- IP C: Contiene datos de carácter especial (según el RGPD, datos médicos, de menores, etc.).

5) ETIQUETADO DE LA INFORMACIÓN

Con respecto a la clasificación de los activos definidos en el actual documento, se consideran los siguientes lineamientos de acuerdo con la manipulación, procesamiento, almacenamiento, transmisión y destrucción de información:

MANIPULACIÓN DE INFORMACIÓN.

- Los documentos con información del tipo “Confidencial” y “Secreta” deben ser controlados por medio de copias perfectamente numeradas o etiquetadas y llevar un registro de las personas que las tienen.
- La copia o transferencia por cualquier medio (electrónico, magnético, en papel) de información de tipo “Confidencial” y “Secreta” debe estar autorizada y controlada por personas específicas.
- Las personas que dispongan de información de tipo “Confidencial” o “Secreta” debe abstenerse de ejecutar por cuenta propio o ajena, directa o indirectamente, las conductas siguientes:
    - Preparar o realizar cualquier tipo de operación sobre los activos de información correspondientes. Se exceptúa la preparación y realización de operaciones cuya existencia constituye, en sí misma, la información privilegiada, así como las operaciones sobre los mismos que se realicen en cumplimiento de una obligación cuando dicha obligación esté contemplada en un acuerdo celebrado antes de que la persona de que se trate esté en posesión de dicha información.
    - Comunicar la información de tipo “Confidencial” o “Secreta” a terceros, salvo en el ejercicio normal de su trabajo, profesión o cargo, siempre que a aquellos a los que se les comunique la información en el ejercicio normal de su trabajo, profesión o cargo, estén sujetos, legal o contractualmente, a obligación de confidencialidad o hayan confirmado que disponen de los medios necesarios para salvaguardarla.
- Toda persona que tenga acceso a información privilegiada, estará obligada a:
    - Salvaguardarla, sin perjuicio de su deber de comunicación y colaboración con las autoridades judiciales y administrativas en los términos de las leyes aplicables.
    - Adoptar las medidas adecuadas para evitar que dicha información pueda ser objeto de utilización abusiva o desleal.
    - Comunicar a su Dpto., cualquier uso abusivo o desleal de la información manejada del que tenga conocimiento.
- En cuanto al marcado o etiquetado de dichos documentos confidenciales deberán etiquetarse con una leyenda ilegible para personal no autorizado en cada una de las páginas, incluyendo su fecha de emisión.
- El Responsable del Sistema, el personal técnico de sistemas y el personal de otros servicios auxiliares tendrán restringido al máximo la posibilidad de acceso a equipos o ubicaciones en los que se almacene información de tipo “CONFIDENCIAL” y “SECRETA”. En el caso de que el acceso por parte de alguna de las personas anteriores resulte imprescindible, el número de personas con acceso deberá ser el mínimo necesario. Dicho acceso deberá registrarse y en caso del personal de un prestador de servicios externos al Ayuntamiento, el contrato de prestación de servicios debe incluir cláusulas que garanticen la confidencialidad de la información correspondiente a la que, en su caso, se haya podido tener acceso durante la prestación del servicio.
- En cuanto a la documentación en formato electrónico, las personas autorizadas no deben usar discos de red de acceso común para el depósito temporal o permanente de documentos tipo “CONFIDENCIAL” o “SECRETA” salvo cuando se garantice que únicamente, dichas personas pueden acceder a la información contenida en ellos. En cuanto a los correos electrónicos que contengan dicha información o que incorporen anexos con información

con este grado de clasificación, es recomendable extraerlos y eliminarlos de los buzones de correo y guardarlos como archivos.

- Las personas autorizadas tendrán máxima precaución para evitar que personas no autorizadas puedan ver los documentos confidenciales mientras estén trabajando con ellos en el equipo. A la hora de imprimir los documentos "CONFIDENCIAL" o "SECRETA" deberá utilizarse una impresora local y no conectada a la red interna. En caso de no disponer de impresoras locales, los trabajos de impresión enviados a impresoras de red, deben ir protegidos con contraseña y se deberán recoger inmediatamente después de su impresión. En cualquier caso, las impresoras deberán encontrarse en zonas de acceso limitado.
- Las Personas Autorizadas evitarán, en lo posible, depositar en mesas o salas de reuniones los documentos tipo "CONFIDENCIAL" o "SECRETA", que deberán guardarse en lugares de acceso restringido (tales como despachos y archivos) y depositarse en archivadores (que, como regla general, deberán permanecer cerrados), cuyas llaves o combinaciones de acceso estarán exclusivamente al alcance de dichas personas. En el caso de que se detectará el riesgo de copias de llaves o códigos de acceso, deberá procederse a su sustitución o cambio.
- Se prohíbe la realización de copias de documentos tipo "CONFIDENCIAL" y "SECRETA", salvo que el Director del Área o el Responsable de Seguridad lo autorice, previa y expresamente, para la entrega de dichas copias a una persona autorizada. Los destinatarios de las copias deberán ser advertidos de la prohibición de realizar segundas copias. Únicamente las personas autorizadas podrán realizar copias de documentos confidenciales. Las copias de un documento confidencial estarán sujetas a los mismos requerimientos de protección y control que el original.

PROCESAMIENTO DE LA INFORMACIÓN.

- Si se procesa información altamente confidencial ("CONFIDENCIAL" o "SECRETA") o con unos requisitos de seguridad en cuanto a integridad de información críticos o de trazabilidad, es preciso cifrar dicha información previo almacenamiento de la misma en los soportes que corresponda, si se manejan de forma electrónica.

ALMACENAMIENTO DE INFORMACIÓN.

- Todos los documentos impresos del tipo "SECRETA" deben conservarse bajo llave o utilizar un código de acceso a la información o PIN dual que permita el acceso a la misma. Se almacenarán, normalmente, en una caja fuerte.
- La información sensible tipo "CONFIDENCIAL" o "SECRETA" refleja la clasificación a la que pertenece sin importar la forma o medio en la que se encuentre a través de una numeración específica que solo entiende la persona o personas que manejan o hacen tratamiento de sus soportes (metadatos o bien numeración específica a nivel de soporte).
- Los documentos "SECRETA" en formato electrónico deberán estar cifrados. A este respecto, se puede considerar que un documento está cifrado si lo está el soporte o ubicación en que esté contenido.
- Si un equipo que contiene información de tipo "CONFIDENCIAL" o "SECRETA" debe sufrir operaciones de reparación o mantenimiento y estás tiene lugar en el puesto de trabajo, el usuario del equipo debe estar presente durante las mismas. Si las operaciones antes mencionadas, requieren el traslado del equipo, pero no afectan al disco en el que están alojados los datos, este deberá ser desmontado y dejado en custodia del usuario quien debe guardarlo bajo llave. Si, por el contrario, las operaciones antes mencionadas requieren el traslado del equipo y requieren o pueden requerir intervención sobre el disco en que estén alojados los datos, el traslado del equipo deberá contar con la autorización expresa del Responsable de Seguridad. Siempre que sea posible, previamente al traslado, deberá eliminarse la información privilegiada del disco.
- Cuando una persona autorizada se ausente de su puesto de trabajo, deberá guardar de forma segura los documentos tipo "CONFIDENCIAL" o "SECRETA".
- Las personas autorizadas evitarán, en lo posible, depositar en mesas o salas de reuniones los documentos tipo "CONFIDENCIAL" o "SECRETA", que deberán guardarse en lugares de acceso restringido (tales como despachos y archivos) y depositarse en archivadores (que, como regla general, deberán permanecer cerrados), cuyas llaves o combinaciones de acceso estarán exclusivamente al alcance de dichas personas. En el caso de que se detectará el riesgo de copias de llaves o códigos de acceso, deberá procederse a su sustitución o cambio.

TRANSMISIÓN DE INFORMACIÓN.

- El envío de documentos con la clasificación "CONFIDENCIAL y SECRETA" debe realizarse por medio de canales seguros de información tales como mensajería privada, correo electrónico cifrado y considerar, llegado al caso,

la entrega personal. Es importante evitar el uso del servicio postal, fax, internet o medios no controlados para su envío.

- Las personas autorizadas emplearán canales seguros (correo cifrado, VPN, FTP seguro, etcétera) para la distribución de documentos confidenciales en formato electrónico y, en particular, no se utilizarán con este fin los discos de red de acceso común, salvo que se garantice que la información contenida en ellos sólo sea accesible por dichas personas.
- Toda la recepción de información sensible debe acusar formalmente un recibo correspondiente para conocer el estado de la transmisión de la información correspondiente.
- La distribución o transmisión, interna o externa, de Información tipo "CONFIDENCIAL" o "SECRETA", se llevará a cabo previa autorización expresa del Responsable de Seguridad.
- El envío físico de información sensible debe hacerse por medio de paquetes debidamente cerrados y que no permitan observar su contenido.
- Los documentos confidenciales en versión impresa deberán transmitirse en sobre cerrado a nombre de la persona autorizada destinataria y con una marca indicando la naturaleza de la información que contiene. El sobre deberá ser de un solo uso. Adicionalmente, deberá enviarse un correo electrónico al receptor indicando que se le va a enviar información, sin indicar su naturaleza y requerirse el envío de un correo electrónico de respuesta por parte del receptor cuando se haya producido la recepción efectiva. La recogida y entrega de los documentos confidenciales con información "CONFIDENCIAL" o "SECRETA" deberá realizarse en mano, evitando depositarla en bandejas o en la mesa del destinatario sin estar este presente.
- En los envíos al exterior, sea a otros edificios de la entidad o no, el transporte de los documentos tipo "CONFIDENCIAL" o "SECRETA" deberá realizarse por personal autorizado y con las suficientes medidas de seguridad para garantizar su transporte seguro. Si el envío es fuera del Ayuntamiento, se deberá realizar a través de mensajero, con albarán de entrega. En cualquier caso, deberá existir un registro de entradas y salidas de este tipo de envíos.
- Durante el proceso de entrega, los documentos confidenciales deberán almacenarse en lugares que cumplan las medidas de acceso y almacenamiento necesarias. En caso de pérdida o robo, se deberá avisar inmediatamente al emisor.
- Se deberá evitar el uso del fax como medio de transmisión de información tipo "CONFIDENCIAL" o "SECRETA". En caso de ser imprescindible su uso, deberá avisarse al destinatario en el momento del envío para asegurarse de que recoge el documento en el mismo momento de su impresión en destino.
- Cuando las personas autorizadas viajen con documentos confidenciales tipo "CONFIDENCIAL" o "SECRETA" (tanto en soporte electrónico como en papel) tendrán la máxima precaución en lugares y transportes públicos (aeropuertos, aviones, trenes, taxis) para evitar el olvido, extravío o robo de los documentos confidenciales e impedir que personas no autorizadas puedan ver su contenido de forma accidental o intencionada.
- En particular, las personas autorizadas deberán mantener los documentos confidenciales bajo su control en todo momento, evitando depositarlos en equipajes que vayan a facturarse, dejarlos en el interior de un vehículo (aunque este permanezca cerrado) o en una habitación de hotel al ausentarse de ella. Si fuera imprescindible dejar los documentos confidenciales en un hotel, se deberá hacer uso de la caja fuerte.
- La Información tipo "CONFIDENCIAL" o "SECRETA" se transmitirá a los externos tan tarde como sea posible de conformidad con las características de la operación de que se trate.
- Con anterioridad a la transmisión de cualquier información tipo "CONFIDENCIAL" o "SECRETA", los receptores externos, deberán suscribir un compromiso de confidencialidad con el Ayuntamiento, salvo cuando el receptor externo esté sometido a un régimen legal o contractual que recoja el deber de confidencialidad. En todo caso, los Receptores Externos serán informados y deberán manifestar, al menos, que conocen:
    - El carácter confidencial de la información transmitida,
    - Las obligaciones derivadas de la normativa aplicable a la Información Privilegiada
    - Las consecuencias de la infracción de dicha normativa, así como que disponen de los medios necesarios para garantizar el carácter confidencial tipo "CONFIDENCIAL" o "SECRETA".
- Se exigirá, asimismo, la firma de dicho compromiso de confidencialidad a aquellos receptores externos con los que se contacte en una fase preliminar y a los que se presenten las líneas generales de una operación para solicitar ofertas de financiación o asesoramiento, aunque finalmente no participen en la misma.
- En todo caso, la transmisión de información tipo "CONFIDENCIAL" o "SECRETA" por un receptor externo, requerirá la autorización previa, por escrito, del Responsable de Seguridad y la firma por el segundo receptor externo de un compromiso de confidencialidad equivalente.

- La Unidad o área podrá condicionar la transmisión electrónica de información tipo "CONFIDENCIAL" o "SECRETA" a los receptores externos a la encriptación de los documentos confidenciales a través de cualquier procedimiento informático que restrinja el acceso a la información a los receptores externos.

DESTRUCCIÓN DE INFORMACIÓN.

- Se realiza la destrucción de documentos o soportes con información confidencial o con información estrictamente confidencial "CONFIDENCIAL" y "SECRETA" que garantice la no reutilización de la información.
- La destrucción de registros e información altamente confidencial es formalmente autorizada por el Responsable de la Información.
- Las personas autorizadas que hayan tenido acceso a información "CONFIDENCIAL" o "SECRETA" deberán destruir cualquier soporte que contenga esta información en el momento en el que haya dejado de ser útil, salvo que exista algún requisito, legal o de negocio, que justifique su mantenimiento. En este sentido, se deberá tener en cuenta no solo que han de destruirse versiones definitivas de los documentos confidenciales, sino también todos los borradores, copias, extractos y demás documentos de trabajo que contengan Información Privilegiada.
- Cuando resulte proporcionado y factible a criterio de la entidad, los documentos confidenciales en formato electrónico deberán eliminarse utilizando herramientas de borrado que garanticen que la información eliminada es irrecuperable.
- En el caso particular de que se retire o se dé de baja un ordenador (que contenga o haya contenido información de tipo "CONFIDENCIAL" o "SECRETA") o se sustituya el disco u otro dispositivo de almacenamiento de datos, éste deberá destruirse de forma que no pueda recuperarse la información almacenada con borrados bit a bit.
- Por su parte, para la destrucción de documentos confidenciales en papel se emplearán los medios dispuestos por el Ayuntamiento a tal efecto, consistentes en destructoras de papel.
- La destrucción de los documentos confidenciales será ejecutada exclusivamente por las personas autorizadas; en particular, no se encomendará la destrucción de documentos confidenciales tipo "CONFIDENCIAL" o "SECRETA" a personas que no estén autorizadas para acceder a ellos. En el supuesto de que en el proceso de destrucción de la documentación participarán agentes externos al Ayuntamiento (por ejemplo, empresas especializadas en destrucción en el caso de destrucción de grandes volúmenes de documentación) en los contratos de prestación de servicio, deberán incluirse cláusulas que garanticen la confidencialidad de la información a la que hayan podido tener acceso dichos agentes externos durante el proceso de su destrucción. Asimismo, se requerirá la expedición de un certificado acreditativo de la destrucción de los documentos confidenciales por parte de los agentes externos.

Para la información pública o de uso público o interno del Ayuntamiento ("PÚBLICA O PUBLICABLE" o "USO INTERNO") es preciso realizar los siguientes lineamientos:

- La información del Departamento que se utilice para dar conferencias, discursos o presentaciones abiertas lleva la autorización del dueño de la información y del Responsable que corresponda.
- La información interna del Ayuntamiento que se transfiera o se almacena interna o externamente deberá de controlarse específicamente para que no se distribuya de forma no autorizada e indebida. Las personas con acceso o autorizadas para su tratamiento serán las responsables de los accesos o de las modificaciones realizadas sobre la misma.
- La información pública deberá de controlarse de tal forma que entre la dicha información no se especifiquen datos de otro nivel de clasificación distinto al público.
- El procesamiento de la información de uso interno se realizará por medios seguros bien a través de canales de comunicación o bien a través de soportes con identificación numérica específica de uso interno solo conocida por las personas que realizan el tratamiento de la misma. Los datos se procesarán con meta-datos e identificación electrónica específica.
- La información de uso interno tanto en soporte electrónico como en papel se podrá destruir una vez se haya aprobada o autorizada de forma específica.

6) MANIPULACIÓN DE LA INFORMACIÓN

En este documento se explican los diferentes controles que hay que tomar para evitar pérdidas de información debido a falta de gestión sobre el uso y almacenamiento de la misma.

1. Todo medio con posibilidad de contener información sensible o confidencial será tratado de manera segura tal y como se describe en el documento "NR.11.Gestión de Soportes".
2. Los documentos se almacenarán dependiendo de su clasificación. A mayor confidencialidad mayor seguridad (armario con llave, caja de seguridad, caja de seguridad localizada en un banco o empresa externa, etc.).
3. Toda información confidencial o sensible deberá tener su respaldo correspondiente.
4. Se reducirá al mínimo la distribución de la información confidencial o sensible. Todo dato confidencial o sensible deberá ser sacado del medio removible en el que viniera y será almacenado en una localización segura con listas de control de acceso lo más restringidas posibles. Posteriormente se procederá al borrado seguro del medio temporal.
5. El acceso a la información confidencial o sensible, así como las listas de distribución y permisos de red especiales está controlado por la "NR.28.Gestión de acceso de usuario.docx" y el registro de privilegios se mantiene en los grupos de control de acceso por directorio. Dichos permisos serán revisados por el responsable del servicio tal y como se describe en el documento anterior.
6. Si la información fuera especialmente sensible, el responsable del servicio evaluará junto al responsable del sistema la creación de un nuevo directorio con una ACL aún más restrictiva para el almacenaje de dicha información. Nunca deberá almacenarse en una unidad no segura.
7. Si se requiere al Responsable de Sistemas crear una copia en un medio físico de información confidencial o sensible, el Responsable del Sistema pedirá la autorización al Responsable del Servicio y creará un registro de las copias creadas en el sistema de incidencias.
8. Toda lista de distribución que sea susceptible de recepción de información confidencial o sensible será revisada periódicamente por su responsable tal y como está descrito en "NR.28.Gestión de acceso de usuario.docx".

7) RESPONSABLE DEL CUMPLIMIENTO

La responsabilidad final de la presente normativa y de la clasificación de la información recae sobre el Responsable de la Entidad, que a su vez estará supervisado por el Responsable de Seguridad.

8) 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.

9) REGISTROS/ANEXOS