DIPUTACIÓN DE ALMERÍA

Procedimiento sobre la gestión del almacenamiento de documentos temporales y de trabajo en las carpetas con acceso total a todos los usuarios en los servidores de almacenamiento en red corporativos (nas)

(Ejemplo: \\naspp\Intercambio, \\naspp\Publico, ETC..)

(DIPALME-ENS-LO PD-0001)

(Aprobado Resolución 480 de 05 Abril de 2017)

DIPUTACIÓN DE ALMERÍA

DIPUTACIÓN DE ALMERÍA

ÍNDICE

Fecha de Redacción

Abril 2017

APROBACIÓN

- La propuesta del documento se aprobó en el Comité de Seguridad de fecha 21 de marzo de 2017.

- La aprobación definitiva se realizo en resolución de presidencia numero 480 de 5 de abril de 2017.

- Entrada en vigor el 1 de Mayo de 2017.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en la gestión diaria en todas las dependencias de la Diputación y de la RPC, hace que el 100% de la información que se gestiona tenga su origen en alguno de los Sistemas y/o Equipos TIC instalados en las distintas dependencias, estando dicha información almacenada y gestionada en esos mismos Sistemas y/o Equipos, donde se producirán conflictos y agresiones y donde existen ciberamenazas que atentarán contra la seguridad de dicha información y, por tanto, de nuestra organización.

Por Resolución de Presidencia núm. 2180/2016, de 24 de noviembre, se crea el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DE LA DIPUTACIÓN Y PARA LA RPC. Entre sus funciones está la de proponer la política de seguridad de la información de esta Administración y de la RPC, así como otros documentos que definan las distintas actuaciones a desarrollar dentro del marco legislativo que regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (Real Decreto 3/2010), protección de datos personales (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) y transparencia (Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno y Ley 1/2014 de Transparencia Pública de Andalucía).

Para cumplir con el ENS, la LOPD y la LT, así como con la Política de Seguridad que la Diputación mantenga en vigor, es necesaria la confección de normas, guías y procedimientos que regulen las distintas medidas que se irán implantando de forma paulatina, y para ello se tendrán presentes las Guías del CCN-STIC así como las recomendaciones y guías de la AEPD y de los Consejos de Transparencia Estatal y Autonómico.

1 ÁMBITO DE APLICACIÓN Y FINES

1. El presente procedimiento tiene por objeto establecer las medidas de índole técnico y organizativas necesarias para garantizar la seguridad en la gestión de los documentos temporales y de trabajo en las carpetas con acceso total a todos los usuarios en los Servidores de Almacenamiento (NAS) en la Red Corporativa de la Diputación de Almería. (\\naspp\Intercambio, \\naspp\publico, etc.).

2 NORMATIVA APLICABLE

2. La normativa sobre seguridad de la Información aplicable es:
   - la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)
   - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (RLOPD)
   - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica.
   - Real Decreto 951/2015, de 23 de octubre, de modificación del ENS.
   - Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a información pública y buen gobierno.
   - Ley 1/2014, de 24 Junio, de Transparencia Pública de Andalucía.

3 INTRODUCCIÓN

3. Los documentos y ficheros temporales y los de trabajo que se almacenan en los Servidores NAS en las carpetas con acceso total a todos los usuarios como es el caso de \\naspp\Intercambio y \\naspp\publico, están configuradas para que todos los usuarios tengan acceso a todos los documentos y ficheros que en ellas se almacenen. El objeto de dichas

carpetas es la de proporcionar la posibilidad de intercambio de información entre las distintas Aplicaciones, Servidores y Usuarios que tienen acceso a la Red Corporativa de Almacenamiento (NAS) de la Diputación denominada ALDIP, flexibilizando el acceso a documentos que se generan y que son necesarios para utilizar por otros usuarios y/o aplicaciones.

4. Al posibilitar el acceso de cualquier usuario a toda la información, la seguridad de dicha información es más vulnerable siendo necesario y urgente el establecer un procedimiento para cumplir con los requisitos de seguridad de la LOPD y del ENS.

5. El RLOPD define
   Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

6. La LOPD establece:
   Artículo 9. Seguridad de los datos:
   El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal para evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

7. EL RLOPD establece:
   Artículo 87. Ficheros temporales o copias de trabajo de documentos.
   1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.
   2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

8. EL ENS establece:
   Artículo 21. Protección de información almacenada y en tránsito.
   1. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil

10. EL ENS en el Anexo II establece las medidas de seguridad que se deben establecer, siendo de aplicación para los ficheros Temporales o de Trabajo:
    mp.info.6: Medidas de Protección de la información - Limpieza de Documentos.

11. EL ENS establece las dimensiones de seguridad, para determinar y diferenciar el impacto que una amenaza podrá realizar sobre los activos de una organización en base a una serie de condiciones. Los términos de dimensiones de seguridad, son ampliamente recogidos en todos los aspectos de seguridad de la Tecnologías de la Información (TI) y recogen conceptos fundamentales para el tratamiento de sistemas, servicios y la información. Las dimensiones de seguridad recogidas en el ENS son cinco:
    - Disponibilidad(D). establece la necesidad para que la información y los sistemas se encuentren activos para la prestación de los servicios.
    - Autenticidad (A): para garantizar esta dimensión es necesario que no pueda acceder a la información o a un sistema quien no esté autorizado.
    - Integridad(I): consiste en validar que un objeto o acción son auténticos y que no han sido alterados durante el transcurso del tiempo.
    - Confidencialidad(C): Garantizar que la información o los propios servicios se encuentran salvaguardados sin que se produzcan accesos indebidos, o si se producen que los datos sean ilegibles.

- Trazabilidad(T): Establecer los procedimientos y mecanismos a emplear por una organización, para que se pueda saber qué ha pasado en un incidente, proporcionando los datos necesarios que permitan llevar a cabo un análisis de seguridad.

4 LISTA DE SERVIDORES NAS Y RECURSOS

12. Los servidores NAS y las Carpetas o recursos de almacenamiento a los que se le aplicará este procedimiento son:

Nombre de Servidor NAS	Nombre de la Carpeta/Recurso	Dirección de la Carpeta/ Recurso	Tipo Uso
NASPP	Intercambio	\\naspp\discoe\Intercambio \\naspp\Intercambio	Ficheros Temporales y de Trabajo
NASPP	Publico	\\naspp\discoe\Publico \\naspp\Publico	Ficheros Públicos (Documentación, Normas, Aplicaciones, Ficheros de Instalación, Etc..)

5 NORMAS DE USO DE LOS ESPACIOS TEMPORALES O DE TRABAJO:

13. Solo se almacenarán en estas carpetas/recursos documentos o ficheros cuyo tipo de uso corresponda con el definido para la carpeta/recurso. (Ver tabla del punto 4).

14. No se almacenarán documentos ni ficheros que:
    - Contengan datos de carácter personal.
    - En caso de borrado o pérdida no se puedan generar de forma fácil.
    - Su necesidad de permanencia en estos espacios sea superior a lo establecido en la tabla del ANEXO I.
    - Que sean privados, confidenciales o secretos.

15. El responsable de los documentos y ficheros serán las Dependencias y usuarios que los copien o generen.

16. Los usuarios que hagan mal uso de los documentos y ficheros asumirán la responsabilidad, derivándose, en su caso, las correspondientes sanciones.

17. Los Usuarios solo deben acceder a los documentos y ficheros respecto a los que, según su atribuciones, tengan competencia para su gestión, no accediendo al resto de documentos y ficheros, aun cuando el sistema se lo permita.

6 RIESGOS

18. Externos a la organización son los derivados de la posibilidad de acceso total, con el consiguiente peligro de grabar Programas Maliciosos (Virus, Troyanos, etc...), que puedan alterar la información existente en dichas carpetas como en cualquier otra a las que los usuarios que accedan tengan privilegios de acceso.

19. Externos, posible fuga de información.

20. Internos a la organización, acceso y difusión de documentos y ficheros con información para la que el usuario no tiene autorización aun cuando el sistema se lo permita.

21. Internos, amenaza a la confidencialidad de los Documentos y ficheros.

22. Internos, posible fuga de información.

23. Internos, manipulación y alteración de la información por usuarios no autorizados bien por error o de forma malintencionada.

7 MEDIDAS SE SEGURIDAD A IMPLANTAR

24. Borrado de la información de forma periódica, para cada Carpeta o recurso compartido, según la tabla del Anexo I. Con ello se reducen los riesgos del punto anterior.

25. Auditar periódicamente:
    - La existencia de Documentos o Ficheros con Datos de Carácter Personal.

- La existencia de Documentos o Ficheros privados, confidenciales o secretos.
- La existencia de ficheros que por sus características y contenido no deban almacenarse en estas carpetas.

26. Comprobar periódicamente el cumplimiento de las normas de uso.

27. Realización de copias de Seguridad para garantizar la información en caso de necesidad manifiesta.

8 DIFUSIÓN Y FORMACIÓN:

28. Hacer una difusión de este procedimiento, realizando una gestión de la difusión entre los distintos colectivos de usuarios

29. Establecer acciones de formación en las que se difunda este procedimiento, así como sobre otros procedimientos y normas de seguridad que se vayan implantando.

9 CONCLUSIONES

30. En los sistemas de almacenamiento NAS, existen espacios de almacenamiento o carpetas con una gestión de autorizaciones de acceso para los usuarios que deben acceder a dicha información (ejemplo \\naspp\Departamentos), siendo esta gestión o bien por grupos de usuarios de dependencias o por usuarios individuales. Así si hay información que aun siendo de trabajo o temporal tiene información con datos personales, más confidencial o que necesita un tiempo de almacenamiento temporal superior al establecido en el Anexo I, se deberá almacenar en estos espacios o carpetas y no en las de almacenamiento temporal.

31. Este procedimiento se podrá implantar a las Entidades Adheridas al convenio marco de la RPC que lo soliciten, con las modificaciones necesarias para adaptarlo a sus necesidades.

ANEXO I: TABLA DE CARPETAS Y RECURSOS CON LOS PROCEDIMIENTOS DE BORRADO:

32. En la siguiente tabla se establece las Carpetas o Recursos compartidos que están afectados por este procedimiento, así como las restricciones de uso y los procedimientos para borrado de la información.

Carpeta o Recurso con acceso a todos los Usuarios	Tipo Uso	Restricciones	Procedimiento de Borrado
\\naspp\Intercambio \\naspp\discoe\intercambio	Ficheros Temporales y de Trabajo	- Solo se almacenarán Documentos o Ficheros Temporales y de Trabajo que no contengan datos de carácter Personal y que no sean privados ni confidenciales.	1.- Por el responsable que lo creó, cuando deje de tener utilidad. 2.- Diariamente de forma automática por el Sistema se borrarán todos los Ficheros y Documentos con una antigüedad de más de 7 días (No se borrarán las estructuras de carpetas y subcarpetas creadas)
\\naspp\publico \\naspp\discoe\publico	Ficheros Públicos (Documentación, Normas, Aplicaciones, Ficheros de Instalación, Etc..)	- Solo se deben almacenar documentos que tengan el carácter de público y se deba mantener en el tiempo a disposición de los usuarios de la Red Provincial de Comunicaciones (Documentación, Guías, Aplicaciones, Ficheros de Instalación, Instrucciones y Manuales, etc.). - No podrán almacenarse ficheros con datos de carácter personal, confidenciales, privados.	1.- Por el responsable que lo creó, cuando deje de tener utilidad. 2.- En auditorías por los técnicos de Sistemas, se borrarán los documentos que no cumplan el tipo de uso ni las restricciones, y aquellos que se constate que no son de utilidad.