

POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

(3ª EDICIÓN)

7. Guía de aplicación de conservación



GOBIERNO
DE ESPAÑA

MINISTERIO
DE HACIENDA

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

TÍTULO: 7. Guía de aplicación de conservación

Elaboración y coordinación de contenidos:

Grupo de Trabajo de PGD-e, en el marco del Plan de Acción de Transformación Digital

Impulsa: Grupo de trabajo para la Coordinación de Archivos de MINHAC y Comisión Ministerial de Administración Digital (CMAD)

Dirige: Subdirección General de Información, Documentación y Publicaciones de MINHAC

Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones

Edición electrónica (versión 1): junio de 2020

Disponible esta publicación en el Portal de Administración Electrónica (PAe):

<http://administracionelectronica.gob.es/>

Edita:

© Ministerio de Hacienda

Secretaría General Técnica

Subdirección General de Información, Documentación y Publicaciones

NIPO: 185-20-051-2

© Ministerio de Asuntos Económicos y Transformación Digital

Secretaría General de Administración Digital

NIPO: 094-20-071-2



El presente documento está bajo la licencia Creative Commons Reconocimiento-Compartir Igual versión 4.0 España.

Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra
- Hacer obras derivadas

Bajo las condiciones siguientes:

- Reconocimiento. Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).
- Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Nada en esta licencia menoscaba o restringe los derechos morales del autor.

Esto es un resumen legible por humanos del texto legal (la licencia completa) disponible en:

<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

ÍNDICE

Histórico de versiones del documento	4
1. ANTECEDENTES	5
2. INTRODUCCIÓN.....	6
3. OBJETIVO Y ALCANCE DE LA GUÍA	7
3.1. Qué NO incluye la Guía.....	7
4. ÁMBITO DE APLICACIÓN Y DESTINATARIOS	8
5. CONSERVACIÓN	9
5.1. Normativa de interés.....	9
5.2. Recomendaciones generales	10
5.3. Conservación de firmas electrónicas	11
5.3.1. Cambios previstos en la conservación de firmas electrónicas	12
5.3.2. Aspectos técnicos	13
5.4. Conservación de formatos de documentos electrónicos	15
5.5. Conservación de soportes	17
5.6. Plataformas y servicios comunes de la administración	21
5.7. Foros y mecanismos de colaboración.....	26
6. DEFINICIONES Y ACRÓNIMOS.....	27
6.1. Definiciones.....	27
6.2. Acrónimos	27
7. REFERENCIAS	28
7.1. Legislación	28
7.2. Otros	29
ANEXO I. NORMATIVA	30
ANEXO II. LISTA DE COMPROBACIÓN PARA LA CONSERVACIÓN.....	38
Equipo responsable de la elaboración de la política de gestión de documentos electrónicos.....	43

ÍNDICE DE TABLAS

Tabla 1. Valores de metadatos para una copia autentica con cambio de formato realizada por obsolescencia de formato. Original con estado de elaboración: “Original”, “Copia electrónica auténtica con cambio de formato”, “Copia electrónica auténtica de documento papel” o “Copia electrónica parcial auténtica”16

Tabla 2. Valores de metadatos para una copia autentica con cambio de formato realizada por obsolescencia de formato. Original con estado de elaboración “Otros”17

Tabla 3. Metadatos para la conservación de expedientes y documentos electrónicos en Archive23

Histórico de versiones del documento			
Versión	Nombre del documento	Fecha	Descripción
0	7. Guía de aplicación de conservación	16/07/2019	Versión 0 aprobada por el grupo de trabajo GTPGD-e, en el marco del PATD
1	7. Guía de aplicación de conservación	1/06/2020	Versión 1 aprobada por el grupo de trabajo GTPGD-e, en el marco del PATD

1. ANTECEDENTES

1. En el año 2014 se publicó la [Política de Gestión de Documentos electrónicos](#) del Ministerio de Hacienda y Función Pública (entonces Ministerio de Hacienda y Administraciones Públicas), la primera elaborada en el entorno de la Administración General del Estado. La Política, consensuada entre los diferentes organismos del Ministerio de Hacienda y Función Pública, por el Ministerio de la Presidencia y por la Subdirección General de los Archivos Estatales del Ministerio de Educación Cultura y Deportes, ha servido de referencia para el desarrollo de políticas de gestión de documentos electrónicos posteriores, tanto de la AGE como de las Comunidades Autónomas y Entidades Locales.
2. Pasados seis años desde la publicación de la Política de Gestión de documentos electrónicos, se hacía necesaria una actualización de la misma, sobre todo, teniendo en cuenta las experiencias que se han tenido en administración electrónica en las aplicaciones de tramitación y archivo electrónico. También era necesaria la adaptación a la nueva normativa: la [Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas](#) y la [Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público](#), sin olvidar que en fechas próximas será aprobado el nuevo reglamento de administración electrónica, que desarrollará las dos leyes citadas.
3. En el año 2016 se aprobó la segunda edición de la Política de Gestión de Documentos Electrónicos del entonces Ministerio de Hacienda y Función Pública, que fue galardonada con el premio al mejor proyecto archivístico en el VII Congreso de Archivos de Castilla y León (25-27 de mayo de 2016).
4. [La Política de gestión de documentos electrónicos](#) (tercera edición) recoge pautas para la elaboración de un Plan de Preservación en el que se tratan puntos como los elementos a proteger, los actores involucrados, las medidas aplicables, etc. Además, la Política incluye pautas para la conservación de elementos concretos como firmas electrónicas.

2. INTRODUCCIÓN

5. Esta guía aporta orientaciones para llevar a la práctica el proceso de conservación establecido en la política de gestión de documentos electrónicos ([tercera edición](#)). Se recuerdan aquí por su relevancia para lo que sigue los siguientes tres aspectos que se indican al comienzo del apartado 2.5.7 de la misma:
- La conservación de los documentos y expedientes electrónicos atenderá a los plazos legales y en su caso a los establecidos en el dictamen de la autoridad calificadora y a lo dispuesto en la estrategia de conservación implantada.
 - Atendiendo a lo dispuesto en el Esquema Nacional de Seguridad (ENS), y proporcionalmente a los riesgos a los que estén expuestos los documentos, el Departamento deberá contar con un plan de continuidad para preservar los documentos y expedientes electrónicos conservados, así como sus metadatos asociados, que incluirá lo previsto sobre 'Copias de seguridad (backup) [mp.info.9]', junto con las medidas de protección de la información [mp.info], de protección de los soportes de información [mp.si], y, en cualquier caso, de protección de datos de carácter personal según lo dispuesto en el Reglamento General de Protección de Datos y normativa de desarrollo.
 - De acuerdo con el Esquema Nacional de Interoperabilidad, el desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos se concretará en un programa de tratamiento específico para la gestión de documentos y expedientes electrónicos que se aplicará de manera continua sobre todas las etapas o períodos de su ciclo de vida, garantizando su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los documentos y su contexto.

3. OBJETIVO Y ALCANCE DE LA GUÍA

6. El objetivo de esta guía de aplicación es desarrollar los conceptos en materia de conservación de documentos y expedientes electrónicos que establece la [Política de Gestión de Documentos electrónicos](#) del Ministerio, en su tercera edición:
 - i. Criterios para la conservación de la firma electrónica.
 - ii. Criterios para la conservación de soportes.
 - iii. Criterios para la conservación de formatos.

3.1. Qué NO incluye la Guía

7. Esta guía aporta recomendaciones o aspectos a considerar por el Ministerio al respecto de la conservación.
8. La guía no pretende ser un manual de los procesos a aplicar para la conservación de documentos y expedientes electrónicos que, como el resto del Sistema de Gestión Documental, deberán desarrollarse de acuerdo con las directrices establecidas en la Política de Gestión Documental aplicable.

4. ÁMBITO DE APLICACIÓN Y DESTINATARIOS

9. Esta guía tendrá su ámbito de aplicación en el Ministerio de Hacienda, y en sus entidades públicas que así lo decidan. Su aplicación en el Ministerio Política Territorial y Función Pública y en el Ministerio de Asuntos Económicos y Transformación Digital, que han participado en los trabajos de elaboración, deberá ser aprobada por dichos departamentos. Dado su carácter global, también puede ser válida y de aplicación en las entidades y organismos del sector público que así lo deseen.
10. Dentro del ámbito de aplicación definido anteriormente, los destinatarios del contenido de esta guía son los siguientes:
 - i. Responsables de gestión, conservación y archivo de documentos y expedientes electrónicos.
 - ii. Desarrolladores de aplicaciones de gestión, conservación y archivo de documentos y expedientes electrónicos.

5. CONSERVACIÓN

11. El Marco Europeo de Interoperabilidad trata la conservación de la información como su decimoprimer principio fundamental, indicando que:

Principio fundamental 11. Conservación de la información

La legislación exige que las decisiones y los datos se almacenen y que se pueda acceder a ellos durante un período de tiempo determinado. Esto significa que los documentos de archivo y la información guardada en forma electrónica por las administraciones públicas a efectos de documentar los procedimientos y las decisiones deben conservarse y deberán convertirse, si es necesario, a nuevos medios cuando los antiguos se queden obsoletos. El objetivo es garantizar que los documentos y otras formas de información conserven su legibilidad, fiabilidad e integridad y que se pueda acceder a ellos durante todo el tiempo que sea necesario conforme a las disposiciones de seguridad e intimidad.

A fin de garantizar la conservación a largo plazo de los documentos electrónicos de archivo y otros tipos de información, deben seleccionarse unos formatos que garanticen la accesibilidad a largo plazo, incluida la conservación de las firmas electrónicas asociadas y otras certificaciones. A este respecto, el empleo de servicios cualificados de conservación, en consonancia con el Reglamento (UE) nº 910/2014, puede garantizar la conservación a largo plazo de la información.

5.1. Normativa de interés

12. Esta sección identifica las normas y articulado de interés para la conservación. En el Anexo I. Normativa, se incluye el texto de los artículos mencionados.
- i. El marco normativo general de la administración electrónica se establece con las Leyes [39/2015](#), de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y [40/2015](#), de 1 de octubre, de Régimen Jurídico del Sector Público
 - ii. El artículo 46 de la [Ley 40/2015](#), Archivo electrónico de documentos, establece requisitos generales para el archivado de documentos electrónicos, haciendo referencia explícita a la aplicación del ENS y la legislación de protección de datos de carácter personal.
 - iii. El artículo 17 de la [Ley 39/2015](#), Archivo de documentos; trata el archivo electrónico de expedientes finalizados.
 - iv. El artículo 156 de la [Ley 40/2015](#), establece la obligada aplicación del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad en la actividad de las Administraciones Públicas y por tanto en lo que respecta a la conservación de documentos electrónicos e información administrativa.
 - v. El artículo 13 de la [Ley 39/2015](#), Derechos de las personas en sus relaciones con las Administraciones Públicas, establece la obligación de la Administración de proteger los datos de carácter personal de los ciudadanos que figuren en sus archivos.
 - vi. La disposición adicional segunda de la [Ley 39/2015](#), obliga a las administraciones públicas a utilizar las plataformas comunes proporcionadas por la Adminis-

tración General del Estado para la implementación de servicios básicos de administración electrónica, entre los que se encuentra el archivo único de documentos requerido por el artículo 17 de esta misma ley.

- vii. El artículo 157 de la [Ley 40/2015](#), Reutilización de sistemas y aplicaciones de propiedad de las administraciones públicas, establece la obligación de reutilizar soluciones existentes en la implementación de nuevos sistemas o mantenimiento de los existentes.
- viii. El artículo 27 de la [Ley 39/2015](#). Validez y eficacia de las copias realizadas por las Administraciones Públicas, establece las condiciones de emisión de copias auténticas por la administración.
- ix. El artículo 41 de la [Ley 40/2015](#), Actuación administrativa automatizada, establece las condiciones para la actuación administrativa automatizada.
- x. Los artículos 42, *Sistemas de firma para la actuación administrativa automatizada* y 43, *Firma electrónica del personal al servicio de las Administraciones Públicas*, de la [Ley 40/2015](#), establecen los medios de firma electrónica utilizados por la administración.
- xi. El artículo 21 del [Real Decreto 4/2010](#), *Condiciones para la recuperación y conservación de documentos*, establece, entre otros requisitos, la necesidad de que los organismos públicos cuenten con una política de gestión documental acorde a [la NTI de Política de gestión de documentos electrónicos](#), que detalle los mecanismos y procedimientos de conservación de expedientes y documentos.
- xii. El artículo 22 del [Real Decreto 4/2010](#), *Seguridad*, exige la aplicación de medidas de seguridad acordes al [ENS](#) y la normativa de protección de datos de carácter personal y la aplicación de una política de firma y certificados coherente con la [NTI Política de Firma y Sello Electrónicos y de Certificados de la Administración](#), siendo esta conforme a elDAS ([Reglamento \(UE\) N° 910/2014](#)).
- xiii. El artículo 23, *Formatos de los documentos*, del [Real Decreto 4/2010](#), junto con las [NTI de documento electrónico](#), [NTI de expediente electrónico](#), [NTI de digitalización de documentos](#) y [NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos](#), cubren aspectos relacionados con el formato de almacenamiento y la accesibilidad a largo plazo de los documentos electrónicos

5.2. Recomendaciones generales

- 13. El desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos de una organización **se concretará en un programa** continuo de gestión de documentos y expedientes electrónicos que abarca todas las etapas de su ciclo de vida.
- 14. El programa de gestión documental **garantizará** en todo momento la autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad de documentos y expedientes, lo que permitirá la protección, recuperación y conservación física y lógica de los documentos y su contexto.

15. La conservación no es un proceso de gestión documental exclusivo de las últimas fases del ciclo de vida de los documentos, sino un proceso que abarca toda su existencia, concretado en la aplicación de medidas de preservación y conservación a los documentos electrónicos desde el momento de su captura por el sistema de gestión de documentos.
16. La conservación y su planificación **deben plantearse** como una parte integral de la política de gestión documental de la organización. Para el desarrollo de un plan de conservación efectivo es necesario que la organización cuente con elementos de la política como un cuadro de clasificación y un calendario de conservación. Pero al mismo tiempo las decisiones sobre conservación, afectarán al desarrollo de muchos aspectos de la política de gestión de documentos, como: los formatos y tipos de firma aplicables a los documentos, la definición del esquema de metadatos y la descripción de documentos, la asignación de roles y responsabilidades y las directrices para la definición de los procesos de gestión documental. Un ejemplo concreto, es la obligación de ingreso de expedientes terminados en el archivo único y la compatibilidad con [Archive](#).
17. Disponer de una política de gestión documental desarrollada en base a un análisis riguroso de las necesidades de la organización permite un uso eficiente de los recursos dedicados a la conservación. La valoración de documentos, su clasificación, calificación y la determinación de los calendarios de conservación, junto a otros aspectos como los requisitos y frecuencia de acceso, asegura que:
 - i. Se conservan los expedientes necesarios, bajo medidas de protección adecuadas a su valor para la administración.
 - ii. No ingresan en el archivo, individualmente o como parte de un expediente, documentos que no es necesario conservar.
 - iii. Los documentos y expedientes ingresan en el archivo en formatos adecuados, firmados y con los metadatos necesarios para su conservación y recuperación del archivo.
 - iv. Los documentos se transfieren a archivos (central, histórico) con características adecuadas a su estado dentro del ciclo de vida.
 - v. Se eliminan, de acuerdo con la normativa y los procedimientos aplicables los documentos que han perdido su valor.

5.3. Conservación de firmas electrónicas

18. La validez a largo plazo de una firma electrónica puede verse comprometida por razones como:
 - i. La caducidad o revocación del certificado utilizado para realizar la firma
 - ii. Debilidades en los algoritmos criptográficos utilizados.
 - iii. Caducidad de los certificados usados en la firma o el resellado.
 - iv. El uso de criptografía para asegurar la confidencialidad de la información, según se establece en la Guía 807 del CNN-Tic Criptología de empleo en el CNS.
19. Según lo indicado en el artículo 22.4 del [Real Decreto 4/2010](#), la conservación de las firmas electrónicas **se realizará** a través del uso de formatos de firma longeva o a través de su conservación y custodia en repositorios y archivos electrónicos, así como de los

metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la política de gestión de documentos.

20. En este sentido es fundamental que los documentos electrónicos generados por las administraciones públicas ingresen en el archivo electrónico único, puesto que su custodia en el mismo asegura que se le apliquen las medidas necesarias para mantener su autenticidad, integridad y conservación a lo largo del tiempo.
21. Para que una firma se considere longeva, según la [Política de firmas de la AGE](#), debe **cumplir las siguientes condiciones**:
 - i. En primer lugar, deberá verificarse la firma electrónica producida o verificada, validando la integridad de la firma, el cumplimiento de los estándares XAdES, CAdES o PAdES, y las referencias.
 - ii. Deberá realizarse un proceso de completado de la firma electrónica, consistente en lo siguiente:
 - a. Obtener las referencias a los certificados, así como almacenar los certificados del firmante.
 - b. Obtener las referencias a las informaciones de estado de los certificados, como las listas de revocación de certificados (CRLs) o las respuestas OCSP, así como almacenarlas.
 - iii. Al menos, deben sellarse las referencias a los certificados y a las informaciones de estado.
 - iv. En caso de almacenar los certificados y las informaciones de estado dentro de la firma se recomienda sellar también estas informaciones, siguiendo los niveles de conformidad “LT o “LTA” de los perfiles Baseline de las firmas AdES, o bien las anteriores modalidades –X o –A de los estándares ADES anteriores a Baseline (para el caso de documentos antiguos cuyas firmas no hubieran sido generadas originariamente con perfil Baseline).
22. Para proteger la firma electrónica frente a la posible obsolescencia de las firmas o certificados de firma, de forma que mantenga su validez la [Política de firmas de la AGE](#) requiere que se siga uno de los siguientes procesos, de acuerdo con las especificaciones técnicas para firmas electrónicas de tipo CAdES, XAdES o PAdES:
 - i. Aplicar un mecanismo de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente.
 - ii. Almacenar la firma electrónica en un depósito seguro, garantizando la protección de la firma contra falsificaciones y asegurando la fecha exacta en que se guardó la firma electrónica (las operaciones de fechado se realizarán con marcas de fecha y hora, no siendo necesario su sellado criptográfico).

5.3.1. Cambios previstos en la conservación de firmas electrónicas

23. En el momento de escribir esta guía, se encuentra en desarrollo una nueva versión de la Política de Firma de la AGE, conforme a la nueva [Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados](#). La nueva NTI se ajusta al [Reglamento \(UE\) no 910/2014](#) del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado

interior» y a la «[Decisión de Ejecución UE 2015/1506](#) de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público»

24. Aunque la nueva NTI no cambia la aproximación general para la conservación y archivado de firmas electrónicas, sí se introducen cambios significativos respecto a los tipos de certificados y sellos electrónicos que debe usar la administración, los formatos y reglas utilizadas en la generación y validación de firmas y los aplicables a sellos de tiempo. Algunos de los cambios incluidos por la nueva NTI son:
 - i. Los formatos utilizados en el archivado y custodia de firmas, cuando las evidencias de validez se almacenen como parte de la propia firma, serán los establecidos por la [Decisión de Ejecución UE 2015/1506](#).
 - ii. Además del resellado y la custodia en repositorios seguro, se admiten otros sistemas que garanticen la preservación de las firmas y sellos a largo plazo con certeza de la comprobación de su validez en el momento más próximo que sea posible respecto a su generación o admisión. Estos sistemas adicionales **deberán estar descritos** minuciosamente en el documento de gestión de política de custodia documental de la entidad, con indicación de los plazos en los que los sistemas estuvieron vigentes y los archivos a los que estos sistemas se aplicaron, especialmente para el caso de valoración documental a largo plazo por especialistas en archivos.
 - iii. Cuando se generen firmas longevas, **se incluirán**, además de los certificados del firmante y su cadena de certificación, la cadena de certificación del sello de tiempo utilizado.
 - iv. Aunque se siguen admitiendo los formatos de firma definidos en la anterior versión de la NTI, se recomienda que las nuevas firmas se realicen utilizando los formatos definidos en la [Decisión de Ejecución UE 2015/1506](#).
25. La adaptación de la [Plataforma @firma](#) y otros servicios comunes a la futura normativa minimizará los cambios requeridos en los sistemas de los organismos públicos que los utilicen.

5.3.2. Aspectos técnicos

26. Según el [Anexo 12](#) de la [Política de gestión de documentos electrónicos](#) **se deben seguir unas recomendaciones** en cuanto al “Tratamiento de las garantías técnicas en relación a la firma electrónica de los expedientes y sus documentos electrónicos archivados definitivamente y en el momento de su pre-ingreso”.
27. Sobre las firmas longevas en expediente electrónico y su ingreso en el archivo.
 - i. El Archivo definitivo de documentación **deberá en todo caso, comprobar** la validez de las firmas electrónicas del índice de los expedientes electrónicos, debiendo ser longeva en el momento de su archivado.
 - ii. La actualización de dicha firma a formatos longevos **deberá hacerse** preferentemente por parte del sistema gestor, aunque podrá realizarse por parte del sistema de archivado.

- iii. **No podrán ingresarse** expedientes con firmas del índice inválidas, antes de su pre-ingreso deberá regenerarse y presentar una firma correcta.

28. Sobre el resellado de expedientes y documentos archivados.

- i. El sistema de archivado **deberá controlar** la validez y tener actualizadas las firmas de los expedientes electrónicos que custodia.
- ii. Será suficiente con el resellado de la firma longeva del índice del expediente electrónico.
- iii. Toda acción dirigida al mantenimiento de la validez de las firmas **deberá quedar reflejada** en el sistema de archivado como trazas asociadas al expediente conservadas permanentemente.

29. Sobre las firmas de los documentos electrónicos en el momento del ingreso:



- i. **Se recomienda** que los documentos electrónicos que forman parte de un expediente electrónico se ingresen en el archivo con formatos longevos de firma.
- ii. Aquellos **documentos electrónicos que presenten firmas válidas en formatos no longevos**, podrán:
 - a. Ser archivados con la firma original, al considerarse que la firma longeva del índice garantiza su integridad y validez.
 - b. Que el sistema de gestión convierta la firma a formatos longevos antes de su remisión al archivo definitivo, actualizando el índice del expediente del que forma parte cuando sea necesario.
 - c. Que el sistema de archivado convierta la firma a formato longevo, como parte del archivo definitivo del expediente. En este caso, el sistema de archivado deberá regenerar el índice del expediente original para reflejar los cambios en las funciones resumen de los documentos.
 - i. el SIP almacenará el expediente y documentos electrónicos originales remitidos por la aplicación, que será distinto al AIP archivado definitivamente
 - ii. Serán iguales en contenido, pero distintos en los metadatos de las firmas.
- iii. Aquellos **documentos electrónicos que, formando parte de un expediente, presenten una firma inválida o no estén firmados**:
 - a. Si el expediente no presenta algún otro documento con firma válida que lo referencie y que pueda otorgarle validez jurídica (como, por ejemplo, un justificante de registro):
 - i. Si se tiene garantía por parte del sistema gestor de la validez del mismo, deberán ser firmados o sellados antes de su ingreso.
 - ii. Si no se tiene dicha garantía, deberá considerarse la conveniencia o no de su inclusión como parte del expediente electrónico. En caso afirmativo, se recomienda esclarecer este extremo mediante metadatos adicionales que expliquen dicha circunstancia.

- i. Se deberá consignar el metadato obligatorio “Estado de Elaboración” con EE99 (Otros)
 - ii. Se deberá consignar un metadato adicional “Comentario”, indicando este extremo de falta de referencia de integridad.
 - b. Si el expediente presenta algún documento electrónico con firma válida que lo referencie, podrán ser mantenidos en su formato inicial, indicando en las estructuras de metadatos adicionales del documento que están refrendados en otro documento, debiendo, en su medida, identificar el mismo.
 - i. Se deberá indicar en el metadato Estado de Elaboración “Otros” (EE=99)
 - ii. Se deberá consignar en metadatos adicionales, “Comentario”, este extremo de ser referenciado en otro documento.
 - iii. En este sentido, se debe considerar por parte de las distintas administraciones, la generación de justificantes de registro con sello electrónicos en formatos longevos, o en su caso, la actualización de los mismos por parte de los sistemas gestores.
30. Sobre la transferencia de expedientes y la relación del proceso con la firma electrónica:
- i. En los procesos de transferencia de expedientes, sin perjuicio de lo que se defina en normativas que afecten a dicho proceso, se deberá realizar el resellado del expediente antes de su remisión al siguiente archivo, teniendo en cuenta las consideraciones previstas en los puntos anteriores
31. Las plataformas @firma y TS@ proporcionan la funcionalidad necesaria para la realización de firmas longevas, la promoción a firmas longevas de firmas realizadas en formatos básicos y, en caso de ser necesario, la aplicación de los sellos de tiempo necesarios para la conservación a largo plazo de las firmas electrónicas presentes en los expedientes y documentos, realizados de acuerdo a la Política de Gestión de Firma Electrónica de la AGE. La Guía Rápida de aplicación de la política de firma electrónica de la AGE y el Manual de Uso de los Servicios de Firma Electrónica de la Plataforma @firma proporcionan información adicional.

5.4. Conservación de formatos de documentos electrónicos

32. Al igual que ocurre con las firmas, la evolución de la tecnología puede hacer que el contenido de los documentos electrónicos resulte inaccesible a medida que cambian los formatos utilizados para su representación. Aún en el caso de que un estándar evolucione a través de versiones que proporcionan “compatibilidad hacia atrás”, de forma que las nuevas versiones de lectores puedan presentar información de versiones antiguas, esta capacidad suele mantenerse por un número limitado de versiones.
33. El artículo 23.3 del [Real Decreto 4/2010](#), Formato de documentos, establece que la administración aplicará una estrategia de conservación de formatos basada en la conversión desde formatos antiguos a otros actuales y adecuados al contenido particular del documento. Esta conversión debe realizarse de acuerdo con los requisitos establecidos en las leyes [39/2015](#), [40/2015](#), [NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos](#) para la generación de copias electrónicas auténticas con cambio de formato.

34. La [NTI del Catálogo de Estándares](#) establece los formatos aceptados para los tipos de contenido más habituales. El catálogo asigna un estado a cada uno de los estándares que recoge (Admitido o en Abandono) que deberá tomarse en consideración tanto para la generación de nuevos documentos como para la planificación de las conversiones de formato necesarias por motivos de conservación.
35. Especialmente, si la organización utiliza formatos no incluidos en el catálogo de estándares, deberá prever en su estrategia de conservación los mecanismos necesarios para la monitorización y gestión de la obsolescencia de formatos y asegurarse de que se cuenta con los procesos y recursos necesarios para acometer los cambios de formato necesarios. En casi cualquier situación práctica, el volumen de documentos a transformar requerirá que los cambios de formato se apliquen de forma automática a los documentos archivados.
36. [Archive](#) permite la invocación de un servicio externo de cambio de formato sobre los documentos archivados. En el momento de escribir esta guía, no se dispone de servicios comunes de cambio de formato.
37. La [NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos](#), establece los valores que deben asignarse a ciertos metadatos de la copia auténtica con cambio de formato. Como regla general, el valor de metadatos obligatorios y complementarios de la copia mantendrá los del original cuando el proceso de copiado auténtico se realiza por motivos de conservación de formato. **Debe prestarse atención a la asignación del metadato “Estado de elaboración”**, distinguiendo los casos en los que el documento a copiar posee calidad de original o copia auténtica, como se recoge en las siguientes tablas.



Tabla 1. Valores de metadatos para una copia auténtica con cambio de formato realizada por obsolescencia de formato. Original con estado de elaboración: “Original”, “Copia electrónica auténtica con cambio de formato”, “Copia electrónica auténtica de documento papel” o “Copia electrónica parcial auténtica”

METADATO	VALOR
Órgano	Identificador normalizado de la organización que realiza la conversión del documento electrónico.
Estado de elaboración	<i>‘Copia electrónica auténtica con cambio de formato’.</i>
Identificador del documento origen	Identificador del documento origen al que corresponde el documento convertido, siguiendo la siguiente estructura: <i>ES_<Órgano>_<AAAA>_<ID_específico></i>
Resto de metadatos obligatorios y metadatos opcionales	Como regla general, y siempre que no se diga otra cosa en la política de gestión documental aplicable, se asignará el valor del metadato correspondiente del documento sobre el que se realiza la copia.

Tabla 2. Valores de metadatos para una copia autentica con cambio de formato realizada por obsolescencia de formato. Original con estado de elaboración “Otros”

METADATO	VALOR
Órgano	Identificador normalizado de la organización que realiza la conversión del documento electrónico.
Estado de elaboración	‘Otros’
Identificador del documento origen	Identificador del documento origen al que corresponde el documento convertido, siguiendo la siguiente estructura: <i>ES_<Órgano>_<AAAA>_<ID_especifico></i>
Resto de metadatos obligatorios y metadatos opcionales	Como regla general, y siempre que no se diga otra cosa en la política de gestión documental aplicable, se asignará el valor del metadato correspondiente del documento sobre el que se realiza la copia.



38. Aunque la conversión de formato de grandes volúmenes de documentos se realice de forma masiva mediante un proceso automatizado, **deberán implementarse los controles necesarios** para garantizar que el proceso es el adecuado, que se aplica correctamente y que las copias generadas son fieles al contenido original y el nuevo formato y la calidad de la copia permiten su conservación durante el resto de la vida útil del documento.
39. Siempre que sea posible y especialmente en documentos que requieran periodos de conservación largos, **se optará por conversiones de formato que no introduzcan degradaciones** en la calidad de los contenidos copiados.
40. El cambio de formato hará que se modifique la huella digital incluida en el índice del expediente, por lo que **será necesario** su reconstrucción.

5.5. Conservación de soportes



41. Con el objetivo de garantizar su disponibilidad y accesibilidad, independientemente de la fase del ciclo de vida, los documentos electrónicos **se conservarán** en sistemas de almacenamiento que permitan independizar los soportes de almacenamiento de los servidores que se encargan de gestionarlos. Esta independencia entre servidores y soportes es una medida de protección básica frente a fallos técnicos o indisponibilidad de los servidores y proporciona otras funcionalidades como alta disponibilidad, redundancia de los datos, replicación, etc., que son esenciales para la conservación. **Se evitará**, pues, conservar el documento electrónico en dispositivos móviles, otros equipos de usuario o soportes locales de servidores. Esto no impide obviamente el acceso a los documentos electrónicos desde estos dispositivos o servidores.
42. Los requisitos de acceso al documento electrónico varían en función de la fase del ciclo de vida en la que se encuentre, por lo que los sistemas de almacenamiento que lo alojen

en cada momento **deberán reunir** las características de rendimiento y capacidad adecuadas a dicha fase. Por ejemplo, durante la fase de tramitación, el sistema debería proporcionar un acceso inmediato a los documentos electrónicos. En una fase posterior los sistemas de almacenamiento, sin perjuicio de que continúen garantizando la disponibilidad y accesibilidad de los datos conservados, podrían disponer de características menos exigentes en cuanto a su tiempo de acceso.

43. El tiempo de acceso y capacidad de los sistemas de almacenamiento depende de varios factores:

- i. De las funcionalidades que implemente cada sistema en particular.
- ii. Del tipo de soporte empleado. Los más habituales, en orden de rendimiento decreciente, son: dispositivos de estado sólido (SSD), discos duros magnéticos (HDD) y cinta magnética. Los soportes SSD y HDD permiten un acceso en línea, mientras que las cintas magnéticas suelen emplearse para copias de seguridad o para almacenar datos a los que no se suele acceder.
- iii. Del tipo de interfaz de acceso a los soportes (Thunderbolt, SCSI, FC, ATA, SAS, etc.)
- iv. Del tipo de acceso a estos sistemas. Por ejemplo, los servidores de ficheros o NAS proporcionan en principio un tiempo de acceso mayor que los servidores con almacenamiento en redes SAN. Igualmente, el tiempo de acceso variará en función de si estos sistemas residen en instalaciones propias, sea almacenamiento tipo NAS o SAN, o ajenas (almacenamiento en cloud).
- v. De la implementación de la capa de datos de los sistemas de información que gestionan documentos electrónicos. Estos pueden almacenarse básicamente en bases de datos o en sistemas de ficheros. En función de su configuración las primeras podrían proporcionar un rendimiento mayor y un tiempo de acceso menor.

44. Al planificar, diseñar e implementar sistemas de gestión de documentos electrónicos **deberá tenerse en cuenta la adopción de medidas de protección** frente a:

- i. La obsolescencia tecnológica (tanto de soportes o sistemas de almacenamiento como de las aplicaciones que gestionan los documentos electrónicos).
- ii. La degradación o pérdida de datos por corrupción de datos, manipulación inadecuada, daños causados por fuego o inundaciones, ataques intencionados y otras amenazas.
- iii. La degradación por uso de los soportes o fallo de los mismos. Hay que tener presente que cada soporte tiene una vida útil estimada por los fabricantes (en condiciones óptimas de conservación y mantenimiento): número de ciclos máximo de escritura para cada dispositivo SSD, 3-5 años para los HDD, 20-30 años para cintas magnéticas.

45. **En cuanto a la obsolescencia de los soportes de almacenamiento, las medidas a considerar** incluyen:

- i. Refresco o renovación: realizar copias en el mismo tipo de soporte, antes de llegar al final de la vida útil.
- ii. Migración: hacer una copia del contenido de un soporte a otro tipo distinto, o de un sistema de almacenamiento a otro.



- iii. RPO (*Recovery Point Objective*). Definir el tiempo de respuesta necesario ante un ataque y también la frecuencia de realización de copias de seguridad. El RPO se refiere al tiempo máximo aceptable que puede transcurrir entre un incidente que afecte a los datos y el momento en que se realizó la última copia de seguridad de los datos; y, por tanto, a la cantidad de datos que pueda perderse por causa del incidente. Téngase en cuenta que a un menor RPO le corresponderá una mayor frecuencia de copias de seguridad con el consiguiente impacto en recursos dedicados. Tiene relación con el RTO que es el establecimiento de un tiempo de recuperación objetivo o tiempo de interrupción de referencia que mide el tiempo máximo que el servicio puede permanecer interrumpido. Véase para mayor orientación la CCN-STIC 803 ENS. Valoración de los sistemas, el apartado 2.3. 'Criterios para la disponibilidad de los servicios'. El RPO viene determinado por la transaccionalidad del sistema, así como la criticidad del sistema para la organización, es decir, lo mucho que nos importe o no perder dicha información.

46. En relación a la obsolescencia de las aplicaciones deberían mantenerse actualizadas cumpliendo con las recomendaciones de los fabricantes o, si son propias, adoptando los estándares técnicos y buenas prácticas recomendados. En caso de no poder hacerlo es preferible sustituir la aplicación por una nueva antes de que pueda producirse una pérdida de datos.

47. Las **medidas a considerar para la protección de los documentos frente a degradación** por uso habitual y fallos en la tecnología incluyen:

- i. Sistemas RAID que aseguren los datos frente a fallos de los soportes de tipo HDD y SSD.
- ii. El empleo de sistemas de almacenamiento con funcionalidades de alta disponibilidad (doble controlador activo-activo, fuentes de alimentación redundadas, memoria caché con "mirror", etc.) que eviten puntos únicos de fallo y reduzcan las posibilidades de pérdidas de información.
- iii. Redundancia de los documentos mediante replicación:
 - a. La unidad mínima de replicación sería un volumen de almacenamiento, físico o lógico, que contenga documentos electrónicos
 - b. No siempre un soporte de almacenamiento corresponde exactamente con un volumen. Así por ejemplo un soporte de tipo cinta magnética equivale a un volumen físico, mientras que en un sistema de almacenamiento (con soportes de tipo HDD o SDD) pueden existir centenares o miles de volúmenes lógicos.
 - c. En este sentido hay que recalcar la necesidad de tener bien localizados y ubicados los soportes, sean del tipo de sean, que contienen documentos electrónicos.
 - d. En la misma línea podría ser recomendable no mezclar documentos electrónicos y otros tipos de datos no relacionados con ellos en los mismos soportes.
 - e. La replicación, por otro lado, se realizaría siempre entre soportes de la misma naturaleza, en cuanto tipo y capacidad.
 - f. Para realizar las réplicas se emplearían las utilidades que suelen incorporar los mismos sistemas de almacenamiento o software especializado que permita hacerlas.



- g. La réplica, según su ubicación, podría ser de dos tipos:
 - i. Remota, cuando su destino es un sistema de almacenamiento diferente situado en un edificio o ciudad distintos.
 - ii. Local, cuando es el mismo sistema de almacenamiento el que alberga las réplicas.
 - h. Ambas formas de replicación no son incompatibles, por lo que, en función de los recursos disponibles, del valor de los documentos electrónicos y de la necesidad de minimizar los posibles riesgos, podría ser recomendable combinarlas.
 - i. Aun así, sería preferible disponer, como mínimo, de una réplica remota.
 - j. Otro aspecto a determinar sería el número de réplicas que se consideran necesarias y su periodicidad. En este sentido habría que tener presente que las réplicas en disco, al ser más rápidas que las que se hacen a cinta magnética, por ejemplo, suelen reescribirse.
- iv. Copias de seguridad que permitan la recuperación de los documentos electrónicos en caso de pérdida o degradación de datos o desastre de los sistemas. Se diferencian de las réplicas en cuanto permiten copias parciales o completas, restaurar los datos como se encontraban en un momento dado del tiempo y en que suelen disponer de un período de retención, que una vez sobrepasado supone la eliminación automática de esas copias. Es recomendable realizar dos copias de seguridad simultáneas, efectuarlas cuando cambien los datos, almacenarlas en edificios o ciudades distintos, y conservarlas el tiempo que se considere oportuno para garantizar la recuperación de los documentos electrónicos.
 - v. En cuanto a soportes de cinta magnética, almacenamiento en condiciones ambientales controladas (armarios ignífugos, humedad, temperatura, etc., según recomendaciones de los fabricantes de los mismos soportes).
 - vi. Para documentos electrónicos digitalizados, en su fase semiactiva o inactiva, contar con un conjunto denominado "fichero maestro", en un formato considerado longevo (como TIFF, por ejemplo), a partir del cual se obtendrían las copias de consulta.
 - vii. Realizar comprobaciones periódicas y acciones de mantenimiento de los distintos soportes, especialmente los de cinta magnética, para asegurarse de que mantienen todas sus propiedades y no presentan ningún tipo de degradación previa al final de su vida útil esperada.
48. Atendiendo a lo dispuesto en el Esquema Nacional de Seguridad (ENS), y proporcionalmente a los riesgos a los que estén expuestos los documentos, el Departamento **deberá contar** con un plan de continuidad para preservar los documentos y expedientes electrónicos conservados, así como sus metadatos asociados, que incluirá lo previsto sobre 'Copias de seguridad (*backup*) [mp.info.9]', junto con las medidas de protección de la información [mp.info], de protección de los soportes de información [mp.si], y, en cualquier caso, de protección de datos de carácter personal según lo dispuesto en la normativa de protección de datos.
49. Aunque los otros aspectos de la conservación de documentos (conservación de firmas y conservación de formatos) tienen un indudable componente tecnológico, es al tratar la conservación de soportes donde suele relacionarse la conservación de documentos con aspectos de buena gestión de los sistemas de información y la infraestructura TIC. No puede plantearse la conservación de documentos electrónicos si no se dispone de una

infraestructura TIC alojada en dependencias acondicionadas, protegida y gestionada por personal especializado teniendo en cuenta aspectos de: seguridad, mantenimiento, gestión de incidentes, gestión de la configuración, gestión de la capacidad o continuidad del servicio, entre otros. Entre los objetivos de la AGE para la racionalización del uso de recursos se encuentra la transición hacia un modelo de Centros de Proceso de Datos compartidos que actúen como nodos de consolidación TIC. En aquellos casos en los que no resulte adecuado el uso de soluciones disponibles en modo servicio (SaaS, IaaS) y sea necesario el uso de soluciones basadas en equipos dedicados, se optará por su alojamiento en CPD existentes y de acuerdo con los planes de consolidación de infraestructuras aplicables.

5.6. Plataformas y servicios comunes de la administración

50. De acuerdo a lo establecido por la disposición adicional segunda de la [Ley 39/2015](#) al respecto de plataformas y registros de uso común, la Secretaría General de Administración Digital, ha puesto a disposición de las Administraciones Públicas la solución de archivado definitivo de expedientes y documentos electrónicos [Archive](#). La solución facilita la implantación del archivo digital único exigido en el artículo 17 de la [Ley 39/2015](#), Archivo de documentos.
51. La disposición adicional segunda de la [Ley 39/2015](#) establece el uso obligatorio de [Archive](#) o, en casos excepcionales, la interoperabilidad con [Archive](#) de otros sistemas de archivo único cuya necesidad se haya justificado en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.
52. [Archive](#) es un sistema de gestión y preservación de archivo definitivo de expedientes electrónicos conformados de acuerdo al [Esquema Nacional de Interoperabilidad](#) que correspondan a procedimientos finalizados.
53. El funcionamiento de [Archive](#) se ajusta a los requisitos de la Política de Gestión de Documentos Electrónicos e incorpora los mecanismos de configuración y adaptación necesarios para adecuar su funcionamiento a las políticas de gestión de documentos electrónicos de otros organismos públicos. Las funcionalidades y posibilidades de adaptación que ofrece [Archive](#) incluyen:
 - i. Alta y descripción de series documentales mediante la asignación de metadatos para la gestión de procesos.
 - ii. Creación y mantenimiento del cuadro de clasificación de series documentales.
 - iii. Gestión de los metadatos de la política de gestión de documentos de la organización.
 - iv. Aplicación de calendarios de conservación: eliminación y transferencia de documentos, mediante la generación de alertas
 - v. Validación, preingreso e ingreso de expedientes.
 - vi. Selección y gestión de muestras para su conservación permanente.
 - vii. Generación de copias auténticas en papel y con cambio de formato.
 - viii. Conservación de firmas longevas, resellado del índice de los expedientes para la conservación de la integridad a largo plazo.

54. La operativa de [Archive](#) en lo que respecta a la conservación de documentos, incluye los siguientes procesos automáticos:
- Conservación de firmas.** Cada noche, el servicio de resellado automático revisa las firmas de los expedientes archivados (firma de los índices, tal y como indica el anexo 12 de la [Política de gestión de documentos electrónicos](#)) y hace un resellado de las que están a menos de un mes de caducar.
 - Conservación de formatos.** [Archive](#) puede invocar un servicio externo de cambio de formato sobre el contenido de los documentos almacenados. En el momento de escribir esta guía todavía no está disponible un servicio común que pueda realizar los cambios de formato necesarios de acuerdo con la evolución de la [NTI del Catálogo de Estándares](#) y los criterios establecidos en la política de gestión documental y la estrategia de conservación.
 - Conservación de soportes.** La conservación de soporte se realiza como parte de la operación y mantenimiento del sistema por parte de los servicios técnicos de la SGAD, de forma transparente para los usuarios del sistema.
 - Garantías de perdurabilidad.** La base de datos de [Archive](#) está replicada a nivel de sistema de almacenamiento (tipo NAS), en una estructura de directorios y metadatos que permitiría, llegado el caso, poder restaurar el sistema completo partiendo de los datos de la NAS.
55. Es importante que la compatibilidad con [Archive](#) y la reutilización de otras soluciones comunes relacionadas se tome en cuenta, junto con el análisis de necesidades (descripción, clasificación, calificación, requisitos de acceso, calendario de conservación, etc.), desde las primeras etapas del desarrollo de la política de gestión de documentos electrónicos, de forma que se eviten decisiones que dificulten innecesariamente la gestión y conservación de los documentos. Algunos de los servicios comunes a cuyo uso debe tenerse en cuenta son:
- Plataforma @firma.** Proporciona servicios de firma electrónica ajustados a la Política de Firma Electrónica y Certificados de la AGE (Política Marco). Incluye un servicio de promoción de firmas realizadas con perfiles básicos a perfiles longevos.
 - TS@.** La plataforma de sellado de tiempos proporciona servicios de sellado, validación y resellado de sellos de tiempo.
 - Inside.** Es un sistema para la gestión de documentos y expedientes electrónicos que cumple los requisitos para que ambos puedan almacenarse y obtenerse según el ENI.
 - Esquema de Metadatos para la Gestión del Documento Electrónico.** El [eEMGDE](#) incluye los metadatos mínimos obligatorios, definidos en las normas técnicas de interoperabilidad de Documento electrónico y Expediente electrónico, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónico.

[Archive](#) utiliza el esquema de metadatos [eEMGDE](#). La siguiente tabla muestra los metadatos asociados a la conservación que maneja [Archive](#), estos metadatos se aplican a una serie documental y son heredados por todos los documentos y expedientes que forman parte de ella. [Archive](#) permite la conservación de los metadatos obligatorios de ENI y de los metadatos adicionales asignados a documentos y expedientes de acuerdo con el esquema de metadatos de la entidad origen.

Tabla 3. Metadatos para la conservación de expedientes y documentos electrónicos en Archive

METADATO	TIPO	DESCRIPCIÓN	COMO CUBRIRLO
eEMGDE2.1 –Identificador –Secuencia Identificador	Obligatorio	Identificador del procedimiento	Indicar el Código SIA, la Clasificación de ese procedimiento.
eEMGDE4.1 - Fechas – Fecha Inicio	Opcional	Fecha de inicio	AAAA-MM-DDTHH:MM:SSEJ: 2016-04-03T09:31:07
eEMGDE1 Categoría	Obligatorio	Se cubre siempre con la palabra "Serie"	Se cubre siempre con la palabra "Serie"
eEMGDE4.2 –Fechas – Fecha Fin	Opcional	Fecha de fin	AAAA-MM-DDTHH:MM:SSEJ: 2016-04-03T09:31:07
eEMGDE8.4 Seguridad –Sensibilidad Datos Carácter Personal	Obligatorio	La sensibilidad se decide teniendo en cuenta los datos incluidos en los documentos y expedientes.	Habrà que indicar alguno de los siguientes valores: No sensible, Datos Personales, Categorías especiales de datos, Datos de naturaleza penal
eEMGDE9.1 –Derechos acceso uso re-utilización - Tipo Acceso	Obligatorio	Indica si el documento se rige por el régimen general de libre acceso o si, por el contrario, está sujeto a alguna de las limitaciones recogidas en la legislación o normativa de aplicación.	Se indicará si el acceso es Libre o Limitado
eEMGDE9.1.1 -código causa limitación	Condicional	Asignar una codificación a la causa de restricción de acceso para facilitar las consiguientes acciones automáticas precisas sobre el documento.	A,B,C,D,E,F,G,H,I,J,K,L,M, N Valores A - La seguridad nacional B - La defensa C - Las relaciones exteriores D - La seguridad pública E - La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios F - La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva G - Las funciones administrativas de vigilancia, inspección y control H - Los intereses económicos y comerciales I - La política económica y monetaria J - El secreto profesional y la propiedad intelectual e industrial K - La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión L - La protección del medio ambiente M - Otros N - Datos personales

METADATO	TIPO	DESCRIPCIÓN	COMO CUBRIRLO
eEMGDE9.1.2 – Causa legal / normativa limitación	Condicional	Referencia de la ley o norma específica que afecta al documento o expediente en cuanto a su régimen de acceso	Ej.: Art. 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria
eEMGDE9.2 – Derechos Acceso Uso Reutilización – Condiciones Acceso Uso Reutilización	Condicional	Se usa para proporcionar información acerca de la calificación del documento respecto a la reutilización de la información que contiene.	Ej.: Los datos contenidos en los expedientes de esta serie documental son reutilizables bajo las condiciones generales que establece el artículo 8 de la Ley 37/2007, de 16 de noviembre.
eEMGDE13.1.1.1- Calificación tipo de valor	Obligatorio	Sirve para conocer cada uno de los valores (administrativo, fiscal, jurídico, etc.) que poseen los documentos.	Habrà que elegir entre: Administrativo, Fiscal, Jurídico, Otros
eEMGDE13.1.1.2 – Calificación Plazo	Obligatorio	Tipo de decisión emitida por la autoridad calificadora que debe aplicarse sobre los documentos a lo largo de su ciclo de vida y una vez realizada su valoración. Modificar este campo puede implicar la actualización de los expedientes en disco.	CP: Conservación Permanente. EP: Eliminación parcial. ET: Eliminación total. PD: Pendiente de dictamen.
eEMGDE13.2.2 -Calificación -Dictamen - Acción Dictaminada	Condicional	Número de dictamen y tipo de selección o muestreo	Ej.: 18/2017. Muestra: un ejemplar por cada tipo de solicitud de cada 5 años, o bien cuando cambie significativamente el formulario. 77/2017. Muestra: un expediente por año. 92/2019. CP de la documentación conservada por la DG de Presupuestos (MINHAC); ET a los 5 años del resto de la documentación en Oficinas presupuestarias y demás unidades.
eEMGDE13.2.3 -Plazo de ejecución de la acción dictaminada	Condicional	Plazo en el que se tiene que ejecutar la acción concreta que se aplica al documento. Esta acción figura en el sub-elemento eEMGDE13.2.2 - Acción dictaminada Modificar este campo puede implicar la actualización de los expedientes en disco.	Plazo en años: 2, 3...
eEMGDE13.3.1 - Fase de Archivo	Obligatorio	Indicación de la fase de archivo correspondiente al momento del ciclo de vida del documento que se transfiere.	Habrà que indicar si es un Archivo Central, Archivo Intermedio o Archivo Histórico.

METADATO	TIPO	DESCRIPCIÓN	COMO CUBRIRLO
eEMGDE13.3.2 - Plazo de Transferencia	Condicional	Plazo de tiempo en que se traspa la custodia de las diferentes fracciones de series documentales, en cumplimiento del calendario de conservación resultante del proceso de valoración documental. El plazo indicado por este metadato se calculará a partir del valor del metadato eEMGDE4.2 - Fecha fin.	Plazo en años: 2, 3...
eEMGDE13.4 – Documento Esencial	Obligatorio	Calificación de un documento como esencial para el desarrollo de las actividades de la organización y que, por ello, debe ser objeto de medidas especiales de protección, que incluyen su duplicado y almacenamiento en un repositorio diferente.	Sí o No
eEMGDE22.2 - Clasificación – Denominación Clase	Obligatorio	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación.	Ej.: Gestión de gastos
eEMGDE3.1 -Nombre -Nombre Natural	Opcional	Nombre real que se da a la entidad. Es útil para nombrar un expediente, documento...	Ej.: Expediente de enajenación de finca en el Polígono 23 de Tembleque (Toledo).
eEMGDE5 - Descripción	Opcional	Se consigna únicamente la información pertinente no incluida en otros elementos	Ej. para un Documento: 'la serie se inició con motivo del cambio de política interna de la organización, y su definición fue realizada, a partir de los informes previos, por...'
eEMGDE12.1 -Puntos Acceso -Termino Punto Acceso	Opcional	Palabra clave que describe el contenido del documento o de la regulación. Aquellos ya existentes elegidos por cada organización, o los elaborados ex profeso por éstas de conformidad con sus necesidades.	Ej.: Farmacia, Urbanismo, Administración de Empresas, Siglo XIX, Guerra de Iraq, Madrid, Ley 39/2015, Clasificación de documentos...
eEMGDE12.2 - Puntos Acceso – Identificador Punto Acceso	Opcional	Condicional: Debe utilizarse si se utiliza una taxonomía (tesauro, índice, lista de autoridades, lenguaje o vocabulario controlado, etc.) para proporcionar un valor al sub-elemento	521.3, 72, 636 (si se estuviera usando, por ejemplo, la Clasificación Decimal Universal).
eEMGDE12.3 - Puntos Acceso - Esquema Punto Acceso	Opcional	Referencia al esquema del que el punto de acceso se ha extraído. eEMGDE12.1 – Término punto de acceso, o eEMGDE12.2 - ID de punto de acceso. Condicional: Debe utilizarse si se utiliza una taxonomía (tesauro, índice, lista de autoridades, lenguaje o vocabulario controlado, etc.) para proporcionar un valor a los sub-elementos.	Listado de materias de la Biblioteca Nacional, Clasificación Decimal Universal, listado de puntos de acceso en la plataforma PARES

5.7. Foros y mecanismos de colaboración

56. La gestión y conservación de documentos electrónicos es un aspecto común al funcionamiento de todas las administraciones y organismos públicos. Además de su tratamiento en el Esquema Nacional de Interoperabilidad y de la disponibilidad de soluciones y plataformas comunes, existen distintos foros y mecanismos de colaboración a través de los cuales se comparten experiencias y buenas prácticas en la gestión y conservación de documentos en el ámbito administrativo, como:
- i. [Foro del documento electrónico](#). Comunidad que surge con el propósito de dar a conocer los avances de las administraciones públicas españolas en el ámbito de la gestión documental, con el ánimo de fomentar la colaboración entre las mismas, así como con el sector privado.
 - ii. Eventos como las [Jornadas sobre Interoperabilidad y Archivo Electrónico](#), organizadas por el anterior Ministerio de Hacienda y Función Pública.
 - iii. Colaboración interadministrativa en el desarrollo de soluciones comunes, a través de las comunidades de usuarios de [Archive](#), reportando problemas, posibles mejoras o aplicaciones y aportando aplicaciones y componentes desarrollados por los organismos usuarios, por ejemplo, componentes especializados de cambio de formato o que implementen otros servicios de adaptación y extensión de [Archive](#).

6. DEFINICIONES Y ACRÓNIMOS

6.1. Definiciones

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

6.2. Acrónimos

AGE: Administración General del Estado

AIP: Archival Information Package.

EIF: European Interoperability Framework

ENI: Esquema Nacional de Interoperabilidad

ENS: Esquema Nacional de Seguridad

IaaS: Infrastructure as a Service

NAS: Network Attached Storage

eEMGDE: Esquema de Metadatos para la Gestión del Documento Electrónico.

SIP: Submission Information Package

SaaS: Software as a Service

TIC: Tecnologías de la Información y las Comunicaciones

7. REFERENCIAS

7.1. Legislación

- i. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
[BOE-A-2015-10566](#)
- ii. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
[BOE-A-2015-10565](#)
- iii. REGLAMENTO (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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
[DOUE-L-00001-00088](#)
- iv. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[BOE-A-1999-23750](#)
- v. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
[BOE-A-2008-979](#)
- vi. 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.
[BOE-A-2010-1330](#)
- vii. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
[BOE-A-2010-1331](#)
- viii. Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.
[BOE-A-2012-10048](#)
- ix. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
[BOE-A-2011-13170](#)
- x. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
[BOE-A-2011-13169](#)
- xi. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documento
[BOE-A-2011-13168](#)

- xii. Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.
[BOE-A-2016-10146](#)
- xiii. REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
[DOUE-L-2015-81816](#)
- xiv. Decisión de Ejecución UE 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público
[DOUE-L-0-0037-00041](#)

7.2. Otros

- xv. Política de gestión de documentos electrónicos del MINHAP
[URL](#)

ANEXO I. NORMATIVA

57. El artículo 46 de la [Ley 40/2015](#), Archivo electrónico de documentos, establece requisitos generales para el archivado de documentos electrónicos, haciendo referencia explícita a la aplicación del ENS y la legislación de protección de datos de carácter personal.

Artículo 46. Archivo electrónico de documentos.

1. Todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible.
2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.
3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados.

58. El artículo 17 de la [Ley 39/2015](#), Archivo de documentos; trata el archivo electrónico de expedientes finalizados:

Artículo 17. Archivo de documentos

1. Cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable.
2. Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.
3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

59. El artículo 156 de la [Ley 40/2015](#), establece la obligada aplicación del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad en la actividad de las Administraciones Públicas y por tanto en lo que respecta a la conservación de documentos electrónicos e información administrativa.

Artículo 156. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

1. El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.
2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

60. El artículo 13 de la [Ley 39/2015](#), Derechos de las personas en sus relaciones con las Administraciones Públicas, establece la obligación de la Administración de proteger los datos de carácter personal de los ciudadanos que figuren en sus archivos.

Artículo 13. Derechos de las personas en sus relaciones con las Administraciones Públicas.

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

- a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.
- b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.
- c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.
- d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.
- e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.
- f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.
- g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.
- h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
- i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

61. La disposición adicional segunda de la [Ley 39/2015](#), obliga a las administraciones públicas a utilizar las plataformas comunes proporcionadas por la Administración General del Estado para la implementación de servicios básicos de administración electrónica, entre los que se encuentra el archivo único de documentos requerido por el artículo 17 de esta misma ley.

Disposición adicional segunda. Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado.

Para cumplir con lo previsto en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración, las Comunidades Autónomas y las Entidades Locales podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas y registros establecidos al efecto por la Administración General del Estado. Su no adhesión, deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

En el caso que una Comunidad Autónoma o una Entidad Local justifique ante el Ministerio de Hacienda y Administraciones Públicas que puede prestar el servicio de un modo más eficiente, de acuerdo con los criterios previstos en el párrafo anterior, y opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad, y sus normas técnicas de desarrollo, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas.

62. El artículo 157 de la [Ley 40/2015](#), Reutilización de sistemas y aplicaciones de propiedad de las administraciones públicas, establece la obligación de reutilizar soluciones existentes en la implementación de nuevos sistemas o mantenimiento de los existentes.

Artículo 157. Reutilización de sistemas y aplicaciones de propiedad de la Administración.

1. Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información.

3. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el directorio general de aplicaciones, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En este directorio constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de Administraciones.

En el caso de existir una solución disponible para su reutilización total o parcial, las Administraciones Públicas estarán obligadas a su uso, salvo que la decisión de no reutilizarla se justifique en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

63. El artículo Artículo 27 de la [Ley 39/2015](#). Validez y eficacia de las copias realizadas por las Administraciones Públicas, establece las condiciones de emisión de copias auténticas por la administración:

Artículo 27. Validez y eficacia de las copias realizadas por las Administraciones Públicas.

1. Cada Administración Pública determinará los órganos que tengan atribuidas las competencias de expedición de copias auténticas de los documentos públicos administrativos o privados.

Las copias auténticas de documentos privados surten únicamente efectos administrativos. Las copias auténticas realizadas por una Administración Pública tendrán validez en las restantes Administraciones.

A estos efectos, la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales podrán realizar copias auténticas mediante funcionario habilitado o mediante actuación administrativa automatizada.

Se deberá mantener actualizado un registro, u otro sistema equivalente, donde constarán los funcionarios habilitados para la expedición de copias auténticas que deberán ser plenamente interoperables y estar interconectados con los de las restantes Administraciones Públicas, a los efectos de comprobar la validez de la citada habilitación. En este registro o sistema equivalente constarán, al menos, los funcionarios que presten servicios en las oficinas de asistencia en materia de registros.

2. Tendrán la consideración de copia auténtica de un documento público administrativo o privado las realizadas, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

Las copias auténticas tendrán la misma validez y eficacia que los documentos originales.

3. Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, así como a las siguientes reglas:

a) Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

b) Las copias electrónicas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización, requerirán que el documento haya sido digitalizado y deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

Se entiende por digitalización, el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra del documento.

c) Las copias en soporte papel de documentos electrónicos requerirán que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor.

d) Las copias en soporte papel de documentos originales emitidos en dicho soporte se proporcionarán mediante una copia auténtica en papel del documento electrónico que se encuentre en poder de la Administración o bien mediante una puesta de manifiesto electrónica conteniendo copia auténtica del documento original.

A estos efectos, las Administraciones harán públicos, a través de la sede electrónica correspondiente, los códigos seguros de verificación u otro sistema de verificación utilizado.

4. Los interesados podrán solicitar, en cualquier momento, la expedición de copias auténticas de los documentos públicos administrativos que hayan sido válidamente emitidos por las Administraciones Públicas. La solicitud se dirigirá al órgano que emitió el documento original, debiendo expedirse, salvo las excepciones derivadas de la aplicación de la Ley 19/2013, de 9 de diciembre, en el plazo de quince días a contar desde la recepción de la solicitud en el registro electrónico de la Administración u Organismo competente.

Asimismo, las Administraciones Públicas estarán obligadas a expedir copias auténticas electrónicas de cualquier documento en papel que presenten los interesados y que se vaya a incorporar a un expediente administrativo.

5. Cuando las Administraciones Públicas expidan copias auténticas electrónicas, deberá quedar expresamente así indicado en el documento de la copia.

6. La expedición de copias auténticas de documentos públicos notariales, registrales y judiciales, así como de los diarios oficiales, se regirá por su legislación específica.

64. El artículo 41 de la [Ley 40/2015](#), Actuación administrativa automatizada, establece las condiciones para la actuación administrativa automatizada.

Artículo 41. Actuación administrativa automatizada

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

65. Los artículos 42, Sistemas de firma para la actuación administrativa automatizada y 43, Firma electrónica del personal al servicio de las Administraciones Públicas, de la [Ley 40/2015](#), establecen los medios de firma electrónica utilizados por la administración.

Artículo 42. Sistemas de firma para la actuación administrativa automatizada.

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Artículo 43. Firma electrónica del personal al servicio de las Administraciones Públicas.

1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público.
2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público.

66. El capítulo X del [Real Decreto 4/2010](#), Recuperación y conservación del documento electrónico, establece los principios que deben aplicarse a la conservación de documentos electrónicos en el ámbito de la administración.
67. El artículo 21 del [Real Decreto 4/2010](#), *Condiciones para la recuperación y conservación de documentos*, establece, entre otros requisitos, la necesidad de que los organismos públicos cuenten con una política de gestión documental acorde a [la NTI de Política de gestión de documentos electrónicos](#), que detalle los mecanismos y procedimientos de conservación de expedientes y documentos.

Artículo 21. Condiciones para la recuperación y conservación de documentos.

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:
 - a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.
 - b) La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.
 - c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.
 - d) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.
 - e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.
 - f) El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.
 - g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellos documentos que sean

necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

h) La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

68. El artículo 22 del [Real Decreto 4/2010](#), Seguridad, exige la aplicación de medidas de seguridad acordes al [ENS](#) y la normativa de protección de datos de carácter personal y la aplicación de una política de firma y certificados coherente con la [NTI Política de Firma y Sello Electrónicos y de Certificados de la Administración](#), siendo esta conforme a eIDAS ([Reglamento \(UE\) N° 910/2014](#)).

Artículo 22. Seguridad.

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimiento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

69. El artículo 23, *Formatos de los documentos*, del [Real Decreto 4/2010](#), junto con las [NTI de documento electrónico](#), [NTI de expediente electrónico](#), [NTI de digitalización de documentos](#) y [NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos](#), cubren aspectos relacionados con el formato de almacenamiento y la accesibilidad a largo plazo de los documentos electrónicos.

Artículo 23. Formatos de los documentos.

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones

ANEXO II. LISTA DE COMPROBACIÓN PARA LA CONSERVACIÓN

Lista de comprobación para la conservación de expedientes y documentos electrónicos		
La protección de expedientes y documentos electrónicos es un aspecto más de la protección de los activos de la organización y, en concreto, de la seguridad de la información, aunque por sus particularidades y relevancia en la administración se trate de forma separada. Los pasos a seguir para la protección de documentos y expedientes electrónicos son, básicamente, los mismos que se utiliza para la implantación de sistemas de gestión de la seguridad como los basados en ENS. Este documento se orienta a la conservación de documentos generados durante la tramitación de los procedimientos administrativos, la conservación de otros documentos esenciales para el funcionamiento del organismo deberá tratarse de forma similar.		
Análisis de situación		
Los principales propósitos de la protección de documentos y expedientes son: asegurar que el organismo pueda desempeñar sus funciones y cumplir con la obligación legal de conservación de los documentos.		
☐	¿Se dispone de un catálogo de procedimientos administrativos?	SIA
☐	¿Se dispone de un cuadro de clasificación de documentos coherente con el catálogo de procedimientos?	Guía de la NTI de política de gestión de documentos electrónicos
☐	¿Se ha realizado la valoración y calificación de los documentos y se dispone de un calendario de conservación?	Criterios generales para la valoración de documentos en la AGE
☐	¿Se ha realizado un análisis de riesgos y priorizando las acciones de protección necesarias?	ENS
☐	¿Se dispone de un sistema de gestión de la seguridad conforme a ENS?	ENS
☐	¿Se ha definido el esquema de metadatos de la organización y las reglas de aplicación a los documentos teniendo en cuenta ENI y las necesidades de conservación?	NTI de doc. electrónico NTI de exp. electrónico Manual de usuario de Archive
☐	¿Se dispone de una política de gestión de documentos electrónicos formalmente aprobada?	Guía de la NTI de política de gestión de doc. electrónicos

Gestión de documentos – Transiciones en el ciclo de vida de documentos		
☐	¿Se han establecido de procesos que garanticen la transferencia de expedientes y documentos electrónicos al archivo único de la AGE o en general las transiciones entre las distintas fases del ciclo de vida de los documentos y el calendario de conservación?	
Gestión de documentos – Catálogos y trazabilidad		
☐	¿El sistema de gestión de documentos dispone de catálogos que permitan localizar los documentos gestionados por el organismo y sus copias de seguridad? Incluyendo documentos transferidos, documentos eliminados; documentos activos almacenados en sistemas de ficheros, repositorios de aplicaciones de gestión etc.	
Gestión de documentos – Requisitos de ingreso en el archivo único de la AGE		
☐	¿Se conforman expedientes electrónicos de acuerdo con los requisitos de ENI y Archive? NOTA. Los documentos y expedientes se mantendrán en el sistema de gestión de documentos de la organización en los formatos y condiciones marcados por la política y los procedimientos de gestión documental y de acuerdo a los requisitos (p.ej. para metadatos mínimos) marcados por el ENI, de forma que puedan convertirse a los formatos de intercambio de ENI cuando resulte necesario.	NTI de documento electrónico NTI de expediente electrónico. eEMGDE Manual de usuario de Archive
☐	¿Se firman los expedientes y documentos electrónicos de acuerdo con la Política de firmas y certificados de la AGE y las restricciones particulares de Archive ?	Manual de usuario de Archive Política de firmas de la AGE
☐	¿Se han definido en Archive las series documentales identificadas en el cuadro de clasificación junto con los metadatos de conservación adecuados?	Manual de usuario de Archive
☐	¿Se asocian los expedientes electrónicos a la serie documental correspondiente en el momento de su ingreso en Archive ?	Manual de usuario de Archive

Protección de firmas electrónicas		
☐	¿Se validan y convierten las firmas electrónicas a formatos longevos antes de transferir los expedientes y documentos al archivo único?	Política de gestión de documentos
☐	¿Utiliza sistemas de archivo que garanticen el resellado u otros métodos válidos de conservación a largo plazo? Por ejemplo, Archive .	NTI Política de Firma y Sello Electrónicos y de Certificados de la Administración
☐	En caso de aceptar o utilizar sistemas de firma no basados en certificados para documentos incluidos en expedientes a archivar ¿Se puede deducir su validez de otros documentos firmados incluidos en el expediente o se les añade una firma electrónica basada en certificados para dejar constancia de la validez jurídica del documento antes de su archivado?	Política de gestión de documentos
Protección de formatos		
☐	¿Se utilizan formatos adecuados para la conservación a largo plazo de los documentos electrónicos (p.ej. PDF-A)?	
☐	¿Se utilizan únicamente formatos incluidos en la NTI de Catálogo de estándares? Si no es así, ¿Se han tomado las medidas necesarias para monitorizar la obsolescencia de los formatos utilizados y valorado las implicaciones de la conservación de los documentos (p.ej. mantenimiento de licencias, desarrollo de componentes de cambio de formato ad-hoc para Archive, etc.)?	
☐	Se han establecido reglas para la realización de copias electrónicas auténticas con cambio de formato por motivo de conservación en archivo, respecto a: • Formato de destino y proceso de conversión. • Certificados/Sellos y características de la firma a utilizar • Asignación de metadatos a la copia electrónica generada. • Criterios para la eliminación de copias anteriores realizadas por motivos de conservación.	

Protección de soportes

Los detalles de la protección de soportes y sistemas de almacenamiento utilizados por una organización deben abordarse como parte integrante de los proyectos de adquisición de capacidades o sistemas de almacenamiento de registros electrónicos y adecuarse a sus características particulares y conforme al [ENS](#) y la [Normativa de protección de datos de carácter personal](#).

A continuación, se recogen algunos aspectos generales a tener en cuenta al respecto de la protección de soportes, resaltando la importancia de la existencia de copias de seguridad de los documentos (párrafo 48 de esta guía).

☐	¿La protección y conservación de soportes y sistemas de gestión y archivo de documentos electrónicos se trata en el ámbito del sistema de gestión de seguridad de la organización y de acuerdo con el ENS ¹ ?	ENS
☐	¿Se dispone de catálogos ² que mantengan la trazabilidad entre los documentos electrónicos (expedientes, series documentales) y los soportes o sistemas en los que se almacenan?	
☐	¿La clasificación y medidas de protección aplicadas a los soportes/sistema son conformes al ENS y adecuadas al valor de los documentos que almacena, teniendo en cuenta la fase del ciclo de vida en que se encuentran?	ENS Normativa de protección de datos de carácter personal
☐	Los soportes y sistemas se alojan en contenedores o salas con medidas de seguridad y control ambiental adecuados y conformes al ENS .	
☐	Existen planes de mantenimiento para los soportes o sistemas en los que almacenan los documentos y tienen en cuenta aspectos como: • Roles y responsabilidades en la operación y conservación de los soportes y sistemas. • Procedimientos para el manejo/operación de soportes y sistemas. • Procedimientos rutinarios de y conservación de soportes y hardware. • Procedimiento seguro de aplicación de parches de seguridad y actualizaciones de software.	

¹ En todas sus fases, desde la identificación y valoración de activos a la evaluación, auditoría y mejora de la seguridad.

² Si la organización utiliza herramientas de gestión de la seguridad (p.ej. PILAR para análisis de riesgos) deberá incluirse también el modelo de protección de documentos electrónicos (procedimientos, series documentales, sistemas etc.).

	• Renovación de soportes, equipos y componentes antes de la finalización de su vida útil. • Procedimiento seguro de migración a nuevas versiones de software antes de la finalización del soporte del fabricante. • Renovación de las licencias y servicios de soporte adicionales que puedan resultar necesarios. • Registro de incidentes. • Registro de tareas. • Supervisión y control del programa de mantenimiento.	
☐	En el caso de emplear servicios de gestión o archivado de terceros, los contratos o acuerdos incluyen cláusulas respecto a acuerdos de nivel de servicio, descripciones de los servicios incluyendo los de: mantenimiento, resolución de incidentes, conservación de soportes, formatos y firmas electrónicas; medidas y políticas de seguridad aplicables, conformidad con el ENS y la normativa de protección de datos, etc., que garanticen la conservación de los documentos electrónicos de acuerdo a las políticas de seguridad y conservación de la organización.	
Protección de claves		
☐	En caso de que sus documentos o copias de seguridad se almacenen cifradas ¿Dispone de procesos para la gestión de claves que garanticen su protección y disponibilidad aun en caso de incidentes o ausencia de los empleados encargados de su custodia?	
Protección básica – Copias de seguridad		
☐	¿Realiza copias de seguridad periódicas de los documentos y expedientes bajo su custodia?	ENS
☐	¿Están esas copias almacenadas en salas acondicionadas situadas en ubicaciones distintas a la de los datos originales?	ENS
☐	En caso de realizar algún cambio de formato durante el proceso de copiado de seguridad ¿Aplica las condiciones necesarias para que puedan considerarse copias auténticas?	NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos
☐	¿Se aplican medidas de control de acceso físico y lógico adecuadas a los datos de carácter personal o de acceso restringido contenidos en las copias?	ENS

Equipo responsable de la elaboración de la política de gestión de documentos electrónicos (Plan de acción de transformación digital)

Coordinador	
Gerardo Bustos Pretel	Secretaría General Técnica (MINHAC)
Equipo de redacción	
José Luis García Martínez	Secretaría General Técnica (MINHAC)
Diego Castro Campano	Secretaría General Técnica (MINHAC)
Equipo de revisión técnica	
Miguel Ángel Amutio Gómez	Secretaría General de Administración Digital (MPTyFP)
Laura Flores Iglesias	Secretaría General de Administración Digital (MPTyFP)
Equipo de revisión jurídica	
Heide Elena Nicolás Martínez	Abogacía del Estado (MPTyFP)
Federico Pastor Ruiz	Abogacía del Estado (MINHAC)
Participación en el grupo de trabajo	
Josefina Otheo de Tejada Barasoain	AEAT
Julián Antonio Prior Cabanillas	Dirección General de Gobernanza Pública
Andoni Pérez de Lema Sáenz de Viguera	IGAE
Alejandro Millaruelo Gómez	IGAE
Sonia María Cascales Sedano	Dirección General del Catastro
Mayte González Sousa	Secretaría General de Administración Digital
Laura Cristina Méndez Medina	Secretaría General de Administración Digital
Luis José Megino Collado	Secretaría General Técnica (MINHAC)
María del Carmen Barroso González	Dirección General de Función Pública
Juan Antonio Zapardiel López	Inspección General
Carlos Álvarez Martín	INAP
Álvaro Reig González	INAP
Beatriz Bernáldez Méndez	Parque Móvil del Estado
Rosa María Martín Rey	Secretaría General Técnica
María Teresa Villaizán Montoya	Delegación de Economía y Hacienda de Castilla y León
José Luis Esteban Herreros	MUFACE
Celso Rodrigo de Parada Alonso	MUFACE
Ángel Redondo García	Dirección General de Ordenación del Juego
Julio Perales Díaz	Dirección General de Ordenación del Juego
Francisco Javier Garrido Gómez	FNMT
Jesús Pardo Ballenato	FNMT
Víctor Casado Izquierdo	TEAC
Javier Guerra Casanova	SGTIC
Santiago Vélez Fraga	SGTIC
Elsa Pla Colvin	Secretaría General Técnica (MPTyFP)
José Ignacio Gómez Raya	IGAE