DECRETO xx/2016, de xx de xxx, del Consell, por el que se aprueba la Política de Gestión de Documentos Electrónicos de la Generalitat

Preámbulo

La Administración Pública que se fundamenta en los principios de transparencia, participación y colaboración, también, debe sustentarse en una correcta política de gestión documental. La adecuada conservación de los documentos protege los derechos e intereses de los ciudadanos y, en el caso de la conservación permanente de documentación, se protege la historia de una comunidad autónoma, dependiendo, por tanto, de ella su memoria colectiva. Por otro lado, la documentación correctamente gestionada permite a la Administración evaluar el impacto de sus programas y mejorar los procesos de trabajo.

La Ley 2/2015, de 2 de abril, de la Generalitat, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana tiene como uno de sus objetos principales regular y garantizar el ejercicio del principio de transparencia y el derecho de libre acceso a la información pública, entendida como el conjunto de contenidos o documentos que obren en poder de cualquiera de los sujetos incluidos en el ámbito de aplicación de esta ley y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Esta adecuada gestión documental, en aras de la transparencia, debe de hacerse extensiva a la documentación electrónica. El Decreto 220/2014, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana, establece en su artículo 69 que la administración de la Generalitat aprobará y publicará su Política de Gestión de Documentos Electrónicos, en adelante PGDE-GV.

Dicha política debe cumplir los requisitos establecidos tanto en el Esquema Nacional de Interoperabilidad (ENI) como en el Esquema Nacional de Seguridad (ENS) y en sus normas de desarrollo, así como en la Ley 4/1998, de 11 de junio, de la Generalitat, del Patrimonio Cultural Valenciano, y, en concreto, el Decreto 189/2005, de 2 de diciembre, del Consell de la Generalitat, por el que se regula la Junta Calificadora de Documentos Administrativos (JCDA) y el procedimiento de valoración, conservación y eliminación del patrimonio documental de los archivos públicos. El citado artículo también indica que la Política de Gestión de Documentos Electrónicos incluirá directrices para la asignación de responsabilidades, dependencia orgánica y funcional del archivo electrónico y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos.

El derecho de acceso de los ciudadanos a los documentos de las Administraciones Públicas es un derecho esencial que viene recogido en la citada Ley 2/2015 de la Generalitat. En este contexto, hay que tener muy presentes las enormes posibilidades que ofrece la administración electrónica para el acceso a la información. La Administración cuenta con la gestión de documentos y archivos electrónicos como un elemento básico en la política de transparencia activa y datos abiertos, ya que permite generar y mantener información y datos de calidad y proporcionar herramientas para su descubrimiento, comprensión y reutilización, tal y como dicta la Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público, modificada por la Ley 18/2015, de 9 de julio.

La administración electrónica debe, además, conjugar la transparencia administrativa y el derecho a la información con la protección de otros derechos fundamentales como la intimidad de las personas,

regulada en la ley de protección de datos y su desarrollo posterior, y otras restricciones legales.

Por todo ello, las normas que rigen el acceso a los documentos electrónicos deben estar claramente definidas e implementadas tecnológicamente de forma adecuada en la Administración de la Generalitat y deben establecer los sujetos de acceso (ciudadanos, usuarios internos, otras Administraciones), los objetos de acceso (expedientes y documentos electrónicos, etc.) y las condiciones propiamente dichas en relación con el acceso (público, restringido, secreto), así como los cambios que en dichas condiciones se pudieran producir (plazos, desclasificaciones, etc.).

Por otro lado, para cumplir con el principio de transparencia en la Administración, los documentos y expedientes electrónicos deben ser correctamente localizados e identificados, siendo para ello imprescindible contar con procedimientos obligatorios de asignación de los metadatos necesarios que hagan posible conocer su ubicación y facilitar su uso situándolos en el contexto adecuado.

Los documentos deben ser legibles, independientemente de la tecnología con la que se hayan creado, así como procesables y reutilizables. Además, los medios metodológicos y tecnológicos que se utilicen para la búsqueda, recuperación y consulta de los documentos electrónicos deben estar diseñados de acuerdo con los estándares de usabilidad y accesibilidad.

El ENI establece, en su artículo 21, que las Administraciones Públicas deberán poner en marcha las medidas necesarias que garanticen "el acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización con todo detalle del contenido de los documentos, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión en papel de aquellos documentos que sean necesarios". Por lo tanto, la Generalitat tiene que contar con una correcta política de gestión de documentos electrónicos dentro de la planificación de la Administración electrónica.

La implantación de la PGDE-GV en la Generalitat permite hacer transparente la actividad de los departamentos y sus unidades administrativas, documentar la toma de decisiones, facilitar la rendición de cuentas, ofrecer protección y soporte en caso de conflicto o litigio, facilitar la interrelación con los administrados y otras Administraciones y, por último, mantener la memoria colectiva de nuestra comunidad autónoma. Implica también realizar un análisis de riesgos en relación con la pérdida, destrucción o mala gestión de la documentación electrónica y su consecuente gestión de riesgos que ponga los medios para evitarlos. Las estrategias de gestión de riesgos en materia de PGDE deberán alinearse con las estrategias generales de gestión de riesgos de la Generalitat.

La Política es, asimismo, imprescindible para el correcto cumplimiento de 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, que tienen un impacto relevante en el ámbito de la gestión y el archivo electrónicos de los documentos administrativos.

La *conselleria* competente en materia de cultura, según la Ley 3/2005, de 15 de junio, de la Generalitat, de Archivos, es el órgano directivo del Sistema Archivístico Valenciano, que es el conjunto de órganos, archivos y servicios encargados de la protección, organización y difusión del patrimonio documental valenciano. Dicha *conselleria* ejerce sus atribuciones a través de la dirección general con competencias en materia de archivos, incluyendo las competencias en materia de protección del patrimonio documental, sea cual sea el soporte en el que este se ha generado, incluyendo los documentos y expedientes electrónicos. La citada ley, en su artículo 6.3, indica que *"la preservación de los documentos electrónicos se realizará de forma que se*

garantice que los documentos permanecen completos, tanto en su contenido como en su estructura y su contexto; fiables, en cuanto puedan seguir dando fe del contenido; auténticos, en cuanto que originales que no han sufrido alteración en las eventuales migraciones; y accesibles, en cuanto a su localización y legibilidad".

Asimismo, según la Ley de Archivos, esta *conselleria* ejerce las competencias de la elaboración y aprobación de las normas técnicas y de procedimiento para la gestión de los archivos del Sistema Archivístico Valenciano, así como la dirección de la gestión de los archivos de la Generalitat y la de los archivos de titularidad estatal de gestión transferida a la Generalitat. De la *conselleria* competente en materia de cultura depende también la Junta Calificadora de Documentos Administrativos que dictamina, previa valoración documental, qué documentos de la Generalitat pueden ser eliminados reglamentariamente y qué documentos deben ser de conservación permanente mediante la aplicación de procedimientos de valoración reglados, transparentes y participativos.

Por otra parte, la dirección general competente en materia de Tecnologías de la Información y la Comunicación (TIC) asume las competencias definidas en el Decreto 220/2014, de 12 de diciembre, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana, competencias directamente relacionadas con la aplicación e implantación de esta Política. Entre dichas competencias, se incluye la ejecución de la política y la estrategia de administración electrónica de la Generalitat y, en general, el establecimiento de los estándares y medidas necesarias para garantizar la seguridad, la calidad y la interoperabilidad, exigibles a los sistemas de información de la Generalitat y en las relaciones con las demás Administraciones y con los ciudadanos por medios electrónicos, de acuerdo con el ENI y con el ENS.

Dadas las competencias anteriormente descritas, la dirección general competente en materia de TIC y la dirección general con competencias en materia de archivos tienen especial responsabilidad en articular estrategias para garantizar la integridad, autenticidad, disponibilidad, trazabilidad y contexto de producción de los documentos y expedientes electrónicos, así como de sus metadatos asociados, a lo largo de todo el ciclo de vida de los mismos con el fin de garantizar la conservación de los documentos, en especial de aquellos con valor histórico y patrimonial.

Por todo lo dicho, de conformidad con lo que establece el artículo 69 del Decreto 220/2014, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana, a propuesta del Conseller de Hacienda y Modelo Económico, y previa deliberación del Consell, en la reunión del día xx de xxxx de 2016,

DECRETO

Artículo único. *Aprobación de la Política de Gestión de Documentos Electrónicos de la Generalitat.*

Se aprueba la Política de Gestión de Documentos Electrónicos de la Generalitat, en el marco de las Normas Técnicas que desarrollan el Esquema Nacional de Interoperabilidad, que se inserta a continuación.

DISPOSICIONES FINALES

Primera. *Habilitación para el desarrollo y ejecución del decreto*

Se faculta a la persona titular de la Conselleria de Hacienda y Modelo Económico para dictar las disposiciones que requiera la ejecución y desarrollo de este decreto, en cumplimiento de lo dispuesto en el artículo 65 de la Ley del Consell.

Segunda. *Entrada en vigor*

Este decreto entrará en vigor al día siguiente de su publicación en el Diari Oficial de la Comunitat Valenciana.

Valencia, XX de xxx de 2016

El Conseller de Hacienda y Modelo Económico,
VICENT SOLER I MARCO

El President de la Generalitat,
XIMO PUIG I FERRER

Política de Gestión de Documentos Electrónicos de la Generalitat

1.INTRODUCCIÓN....7
2.POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS....9
2.1.Referencias....9
2.2.Alcance de la Política....9
2.3.Datos identificativos de la Política....10
2.3.1.Período de validez....10
2.3.2.Identificador del gestor de la Política....11
2.4.Roles y responsabilidades....12
2.4.1.Actores....12
2.4.2. Responsabilidades....12
2.4.2.1.Alta dirección....12
2.4.2.2.Responsables de procesos de gestión....13
2.4.2.3.Responsables de planificación, implantación y administración del programa de tratamiento de documentos....13
2.4.2.4.Personal implicado en las tareas de gestión....13
2.4.2.5.Otros recursos humanos implicados....14
2.5.Procesos de gestión documental....14
2.5.1.Captura....16
2.5.2.Registro....19
2.5.2.1.Documentación en soporte no electrónico....19
2.5.2.2.Metainformación del asiento registral y de los documentos anexos....20
2.5.3.Clasificación....20
2.5.3.1.Criterios de formación de expedientes electrónicos y agrupaciones de documentos....20
2.5.3.2.Cuadro de clasificación funcional....23
2.5.3.3.Repertorio de series documentales....24
2.5.3.4.Situación transitoria hasta la elaboración del cuadro de clasificación funcional....25
2.5.4.Descripción....25
2.5.4.1.Orientaciones y requisitos tenidos en cuenta para la construcción de un esquema de metadatos....25
2.5.5.Acceso y trazabilidad....33
2.5.5.1.Requisitos de Seguridad y Acceso....34
2.5.5.2.Requisitos de acceso a la información contenida en la entidad Documento....35
2.5.5.3.Requisitos de seguridad en el acceso a la información contenida en el SGDE/SGDEA....39
2.5.6.Calificación....41
2.5.6.1.Documentos esenciales....41
2.5.6.2.Valoración....43
2.5.6.3.Dictamen....45
2.5.7.Conservación....46
2.5.7.1.Trazabilidad de los documentos electrónicos....49
2.5.8.Transferencia....51
2.5.9.Destrucción o Eliminación....55
2.5.9.1.Pasos previos a la destrucción de la información....55
2.5.9.2.Aspectos técnicos relacionados con la destrucción de la información....57
2.5.9.3.Recomendaciones para la elección del nivel destrucción de la información....58
2.6.Asignación de Metadatos....59
2.6.1.Consideraciones sobre los metadatos mínimos obligatorios....60

2.6.2.Consideraciones sobre los metadatos complementarios....61
2.7.Documentación....61
2.8.Formación....61
2.9.Supervisión y auditoría....62
2.10.Gestión de la Política....62
3.PROCEDIMIENTOS INSTRUMENTALES PARA LA GESTIÓN DE DOCUMENTOS....63
3.1.Protocolo de digitalización de documentos....63
3.1.1.Definición de digitalización....63
3.1.2.Objetivo....63
3.1.3.Protocolo de digitalización de documentos....63
3.1.3.1.Directrices generales de digitalización....63
3.1.3.2.Requisitos técnicos....64
3.1.3.3.Escenarios de captura....65
3.1.3.4.Fases del proceso....66
4. REFERENCIAS....70
4.1.Normativa estatal....70
4.1.1.Normas Técnicas de Interoperabilidad....71
4.1.2.Guías Técnicas de Interoperabilidad....72
4.2.Normativa autonómica....73
4.3.Otros documentos de interés....74
5. SIGLAS Y ACRÓNIMOS....76

1. INTRODUCCIÓN

El Esquema Nacional de Interoperabilidad, regulado por el Real Decreto 4/2010, se define en el mismo como *"… el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deben ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad"*. El ENI establece, en su disposición transitoria primera, la obligatoriedad de su implementación en las organizaciones administrativas.

La Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos, publicada por Resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas, establece los conceptos relacionados con el desarrollo de políticas de gestión de documentos electrónicos por parte de las Administraciones Públicas en el marco de la administración electrónica, incluyendo los aspectos relacionados con su implantación práctica e identificación de los requisitos de la gestión de los documentos electrónicos necesarios para la recuperación y conservación de los mismos, así como los procesos y acciones presentes a lo largo de todo su ciclo de vida.

Para la elaboración de la Política de Gestión de Documentos Electrónicos de la Generalitat se ha seguido lo especificado en el Modelo de Política de Gestión de Documentos Electrónicos. Asimismo, se ha contado como modelos prácticos con el documento de Política de Gestión de Documentos Electrónicos del MINHAP, el documento de Política de Gestión del Documento Electrónico del MECD y la Política de Gestión de Documentos Electrónicos y Archivo Electrónico de la Administración Pública de la Comunidad Autónoma de Canarias.

Hay que destacar los beneficios de la implantación de la Política, entre los que se encuentran una mayor transparencia en la actividad administrativa, un mejor gobierno y una rendición de cuentas más ágil hacia los ciudadanos. Una eficaz gestión de los documentos y expedientes electrónicos generados por la Administración es un elemento clave para llevar a efecto el mandato establecido en la Ley 37/2007 sobre Reutilización de la Información del Sector Público, modificada por la Ley 18/2015, de 9 de julio a nivel estatal y en la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y buen gobierno así como en la Ley 2/2015, de 2 de abril, de la Generalitat, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana.

El presente documento de Política de Gestión de Documentos Electrónicos está abierto a futuras reflexiones y actuaciones y, en esta redacción, se ha dividido en dos grandes bloques: el cuerpo principal, que comprende la introducción y los puntos 2, 3, 4 y 5; y los anexos, que se publicarán en la intranet corporativa de la Generalitat. El documento también podrá ser publicado en el portal web y en la sede electrónica de la Generalitat para facilitar su difusión.

En el cuerpo principal se encuentran las disposiciones de esta Política que, previsiblemente, van a ser más duraderas en el tiempo, por derivar de leyes, reglamentos, estándares internacionales y normas técnicas que han sido formalmente aprobadas con el propósito de que estén vigentes durante un período prolongado. Por otra parte, los anexos recogen aquella información complementaria al cuerpo principal que es más susceptible de modificaciones, sean periódicas o puntuales, y cuya actualización no exige de un proceso formal tan riguroso como para las previsiones del cuerpo principal. En los anexos también se recogen especificaciones técnicas que será necesario ir actualizando debido a la rápida evolución de la tecnología y del mercado para dar respuesta a demandas de información o prestaciones de seguridad en

continuo crecimiento.

Algunos anexos de este documento podrán contener información que debe clasificarse como de “difusión limitada”, debido a que detallan especificaciones técnicas sobre los sistemas informáticos de la organización, cuya revelación pública podría aumentar la exposición a incidentes de seguridad deliberados. Tales anexos se mantendrán intencionadamente en blanco en la versión pública de esta Política. Aquellas personas u organizaciones que necesiten conocer su contenido íntegro deberán solicitarlo a los Gestores de la Política indicados en el apartado 2.3.2.

Las disposiciones normativas, estándares, guías y otras fuentes que se citan en este documento se detallan en el punto 4, Referencias, de modo que se inserta un enlace a su detalle explícito en las partes del documento donde sean citadas.

El camino marcado en este documento, con la flexibilidad que exijan las circunstancias, es una hoja de ruta con las tareas necesarias a desarrollar para adaptar la gestión de documentos y expedientes electrónicos al ENI. Su contenido, cuando menos, agrupa las recomendaciones necesarias para llevar a buen puerto la interoperabilidad, que a su vez lleva aparejada una nueva cultura del trabajo administrativo.

2. POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

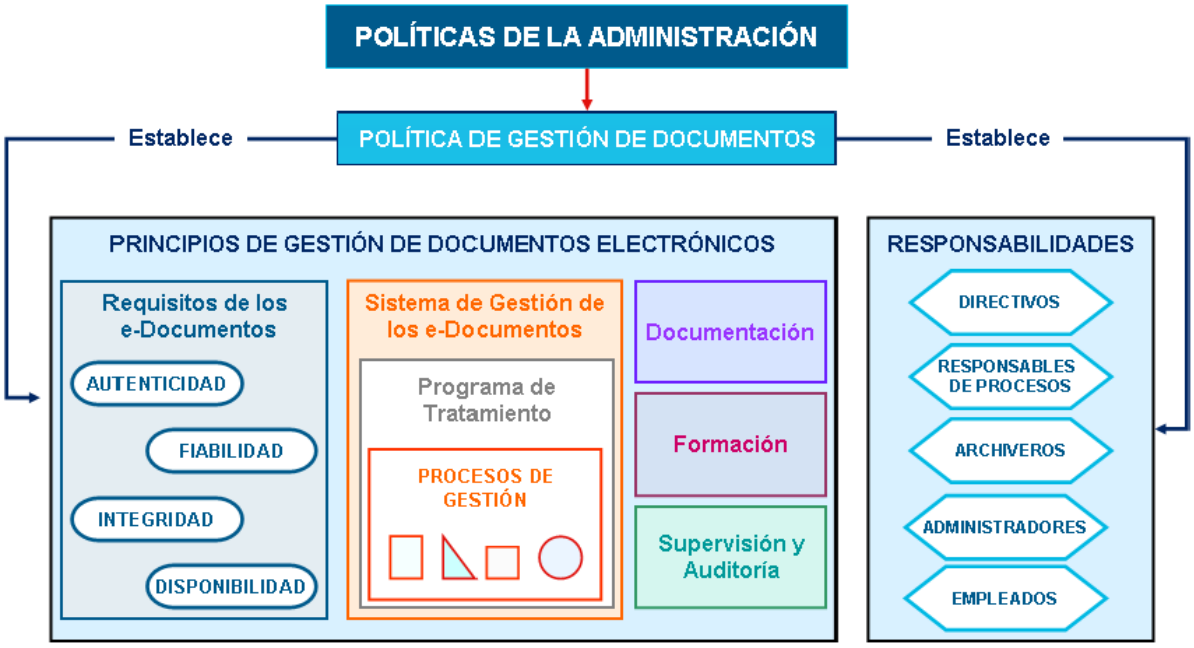
2.1. Referencias

Para el desarrollo del contenido de esta Política, se han tenido en cuenta las normas, buenas prácticas y referencias normativas que se enumeran en el punto 4 de este documento.

2.2. Alcance de la Política

La presente Política de Gestión de Documentos Electrónicos está integrada en el contexto de la organización junto al resto de las políticas implantadas para el desempeño de sus actividades. En particular, esta política está integrada en el marco general de gestión de documentos de la Generalitat, con independencia del soporte en el que puedan estar materializados dichos documentos.

A continuación, se incluye un esquema tomado de la Guía de Aplicación de la Norma Técnica de Interoperabilidad (NTI) de Política de Gestión de Documentos Electrónicos, en la cual se incluye el programa de tratamiento de los documentos electrónicos en el contexto de la Política de Gestión de Documentos de la organización, como el elemento que contempla los procesos de gestión documental:



La Política de Gestión de Documentos Electrónicos de esta organización tiene por objeto establecer el conjunto de criterios comunes asumidos por la Generalitat, así como documentar los mismos, en relación con la gestión de los documentos y expedientes electrónicos producidos o custodiados por los departamentos de la Administración de la Generalitat, sus organismos autónomos y las entidades de derecho público vinculadas o dependientes de la Administración Pública de la Generalitat.

Esta Política de Gestión de Documentos Electrónicos persigue elaborar los requisitos necesarios con el fin de crear, mantener, tratar y conservar documentos electrónicos auténticos y fiables, así como proteger la integridad de los mismos durante todo su ciclo de vida, incluida la fase histórica.

Igualmente, esta Política persigue garantizar la disponibilidad e integridad de los metadatos mínimos obligatorios y, en su caso, los complementarios o necesarios (metadatos de contenido, contexto y estructura) para asegurar la gestión, recuperación y conservación de los documentos y expedientes electrónicos de la Generalitat manteniendo permanentemente su relación.

En particular, se integrará con la política de seguridad que establece el Esquema Nacional de Seguridad, Real Decreto 3/2010, de 8 de enero, y con la normativa propia de la Generalitat, Decreto 66/2012, de 27 de abril, por el que se establece la política de seguridad de la información de la Generalitat y Decreto 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat, puesto que los documentos electrónicos se van a manejar mediante sistemas a los que les es aplicable lo previsto en dicho Esquema y normativa.

A fin de extender la política a entornos híbridos en los que conviven documentos en soportes analógicos y electrónicos, según el Esquema Nacional de Seguridad, se tendrá en cuenta que *"toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos"*.

2.3. Datos identificativos de la Política

Los datos identificativos principales son:

Nombre del documento	Política de Gestión de Documentos Electrónicos de la Generalitat
Versión	1.0
Identificador de la Política [1] y [2]	A10002983_1.0
URI de referencia de la Política	https://sede.gva.es/
Fecha de expedición	17 de octubre de 2016
Ámbito de aplicación	Documentos y expedientes producidos y/o custodiados por la Generalitat

2.3.1. Período de validez

La presente Política de Gestión de Documentos Electrónicos entrará en vigor en la *fecha de expedición* indicada en los Datos Identificativos y será válida hasta que no sea sustituida o derogada por una política o versión posterior. En este caso, se podrá facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar los diferentes sistemas de gestión de documentos electrónicos utilizados por la Generalitat a las especificaciones de la nueva versión.

1 Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común de Unidades Orgánicas y Oficinas (DIR3).

2 Los dos últimos dígitos de este identificador corresponderán con la versión de la política de gestión de documentos electrónicos.

Este periodo de tiempo transitorio deberá indicarse en la nueva versión, pasado el cual sólo será válida la versión actualizada.

Una versión actualizada del texto de la Política, con exclusión de la información indicada en el párrafo séptimo de la introducción, se publicará en la intranet corporativa de la Generalitat. También podrá ser publicada en el portal web y en la sede electrónica de la Generalitat para facilitar su difusión.

Aquellos aspectos que puedan ser actualizables automáticamente, sobre todo en el caso de relaciones por modificaciones normativas, cambios estructurales, etc., serán incluidos en anexos incorporados al presente documento y, en su caso, serán actualizados automáticamente por el gestor del documento sin necesidad de que sea sustituido por una nueva versión.

2.3.2. Identificador del gestor de la Política

Nombre del gestor	Subdirección General de Producción y Consolidación de las TIC Corporativas Subdirección General del Libro, Archivos y Bibliotecas.
Dirección de contacto	C/ Castán Tobeñas,77. Ciudad Administrativa 9 de Octubre-Edif.A sgaae_dgti@gva.es Monasterio de San Miguel de los Reyes Avda. Constitución, 284 servici_arxius@gva.es
Identificador del gestor [3]	A10017895 - Subdirección General de Producción y Consolidación de las TIC Corporativas A10018001 - Subdirección General del Libro, Archivos y Bibliotecas

3 Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común de Unidades Orgánicas y Oficinas (DIR3).

2.4. Roles y responsabilidades

2.4.1. Actores

Los actores involucrados en los procesos de gestión documental contemplados en la presente Política serán los siguientes:

- **La alta dirección** que aprobará e impulsará la política. Serán el titular o los titulares de las *conselleries* competentes en materia de administración electrónica y gestión documental y archivos de la Generalitat.
- **Los responsables de procesos de gestión**, que aplicarán la política en el marco de los procesos a su cargo. Corresponde esta responsabilidad a las personas titulares de los órganos directivos que tienen atribuida por norma la función a la que responden los diferentes procesos y, por delegación de los mismos, a los responsables que reciban dicha delegación.
- **El personal responsable de la planificación, implantación y administración del programa de tratamiento de documentos** y sus operaciones, cualificado, dedicado e instruido en gestión y conservación documental y que participará en el diseño, implementación y actualización de los sistemas de gestión y conservación documental. Esta categoría incluye tanto a archiveros y expertos en gestión documental como a administradores de sistemas y desarrolladores de aplicaciones.
- **Los responsables de las unidades administrativas que gestionen documentos electrónicos**, así como **el personal implicado en dicha gestión**, que aplicará lo establecido en la política a través del programa de tratamiento implantado.

2.4.2. Responsabilidades

A continuación se describen los roles y responsabilidades de los actores antes mencionados:

2.4.2.1. Alta dirección

La alta dirección integrará la política de gestión de documentos con el resto de políticas de la organización. Asimismo, deberá ser consciente de los riesgos que supone una gestión inadecuada de sus documentos.

A partir de unos principios tales como: el enfoque a la ciudadanía y otras partes interesadas; el liderazgo y responsabilidad; la toma de decisiones basada en la evidencia; la implicación del personal; el enfoque sobre los procesos; y el enfoque sistemático de la gestión y mejora continua, trata de:

- Conseguir coherencia en las operaciones para toda la organización.
- Asegurar que los procesos de negocio sean transparentes y comprensibles.
- Garantizar a los consejos de dirección, reguladores, ciudadanos y otras partes interesadas que los documentos se gestionan apropiadamente.

Para la consecución de estos objetivos tiene las siguientes competencias:

- Establecer, mantener y promover la política y objetivos de gestión documental para incrementar la conciencia, motivación y cumplimiento de la organización.
- Asegurar que las responsabilidades y competencias de la gestión de documentos están definidas, asignadas y comunicadas a toda la organización.
- Asegurar que se establece, implementa y mantiene una política de gestión efectiva y eficiente para alcanzar los objetivos de la organización.
- Asegurar la disponibilidad de los recursos y capacitación necesarios para apoyar y mantener dicha política.
- Promover su revisión periódica y decidir e impulsar las acciones de mejora precisas.

2.4.2.2. Responsables de procesos de gestión

Los responsables de procesos de gestión aplicarán la política de gestión de documentos en el seno de la organización y garantizarán el ejercicio de los derechos reconocidos a los ciudadanos. Asimismo, adoptarán las medidas necesarias para la difusión de la Política de Gestión de Documentos Electrónicos y de los procedimientos relacionados con la gestión documental entre todo el personal a su cargo, para que conozca las normas que afecten al desarrollo de sus funciones.

Además, determinarán sus necesidades en cuanto a períodos temporales de utilización de la información, contribuyendo así a la elaboración de las normas de conservación de las series documentales que son fruto de los procesos que gestionan.

2.4.2.3. Responsables de planificación, implantación y administración del programa de tratamiento de documentos

La categoría de personal responsable de la planificación, implantación y administración del programa de tratamiento de documentos y sus operaciones incluye tanto a archiveros y expertos en gestión documental como a administradores de sistemas y desarrolladores de aplicaciones. Los profesionales de la gestión de documentos son responsables de todos los aspectos relacionados con ella, incluidos el diseño, la implementación y el mantenimiento de los sistemas de gestión así como de la formación de usuarios en dicha materia y en las operaciones que afecten a las prácticas individuales.

Los archiveros y expertos en gestión documental, en colaboración con los responsables de los procesos de gestión, llevan a cabo la identificación y valoración documental, establecen los cuadros de clasificación y las normas de conservación de las diferentes series documentales que, posteriormente, serán dictaminadas por las autoridades archivísticas y participan en la planificación e implementación de las políticas y los procedimientos de gestión de documentos.

Los administradores de sistemas serán responsables de garantizar que toda la información sea precisa y legible y que esté a disposición del personal autorizado para acceder a ella siempre que se necesite.

2.4.2.4. Personal implicado en las tareas de gestión

El personal implicado en las tareas de gestión, categoría que incluye a todos los empleados no encuadrados

en las anteriores, son responsables de mantener documentos de archivo precisos y completos sobre sus actividades, de hacer un uso apropiado de los sistemas de información que tratan documentos electrónicos, y de suministrar la información requerida por el Sistema de Gestión Documental a efectos de trazabilidad o cumplimiento de normativa.

2.4.2.5. Otros recursos humanos implicados

La organización puede contar con personal externo a la misma para cubrir una necesidad puntual de la organización (técnicos de empresas externas en el marco de un contrato de servicios con dicha empresa, alumnos en prácticas, becarios, etc.). Todos ellos deben ser informados de los deberes inherentes a crear, mantener y custodiar los documentos electrónicos en el contexto del Sistema de Gestión Documental de la Generalitat.

Los recursos humanos externos deben cumplir con las normas establecidas en las políticas de gestión documental y en el marco legal existente, por ejemplo, protección de datos, confidencialidad sobre información sensible, etc.

2.5. Procesos de gestión documental

El punto V de la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos establece que la gestión de los documentos electrónicos se concretará en un programa de tratamiento específico dentro de la política de gestión de documentos de cada organización.

Según la citada NTI y su guía de aplicación, el programa de tratamiento concretará el diseño, desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos, siendo aplicado de manera continua sobre todas las etapas del ciclo de vida de los documentos y expedientes electrónicos.

Los procesos de gestión que generen documentos y expedientes electrónicos en la organización deben aplicar esta política y el programa de tratamiento de documentos electrónicos que garantice su materialización. Las características y funcionalidades de los sistemas de gestión de documentos se definen a continuación, aclarando previamente que la gestión de documentos electrónicos debe comprender dos momentos:

- Un primer momento, en el que los documentos todavía no han alcanzado su estado definitivo. En esta etapa, los documentos son objetos dinámicos de información, creados mediante diversas aplicaciones, admiten versiones y cambios y está previsto que su información sea compartida. Se controlan y gestionan mediante Sistemas de Gestión de Documentos Electrónicos, en adelante SGDE, si bien estas funciones también pueden llevarse a cabo, en la práctica, por las propias aplicaciones de gestión de procesos.

- En un segundo momento, los documentos han alcanzado ya su forma definitiva, se han integrado en sus respectivos expedientes o agregaciones documentales, han sido provistos de mecanismos que aseguran su autenticidad e integridad, de manera que son inalterables, salvo, en su caso, para añadirles metadatos de gestión y conservación o para corregir errores y se gestionan mediante Sistemas de Gestión de Documentos Electrónicos de Archivo, en adelante SGDEA.

Se recogen a continuación las características y funcionalidades básicas que deben tener los sistemas de gestión de documentos mencionados:

- **SGDE**. Siguiendo las especificaciones de MoReq-2, está orientado básicamente al control, almacenamiento y gestión de la documentación de los archivos de oficina y tiene las siguientes características:
    - Permite la modificación de los documentos.
    - Permite la existencia de varias versiones de los documentos.
    - Puede permitir el borrado de los documentos por parte de sus propietarios.
    - Puede incluir controles de retención de los documentos.
    - Puede incluir estructuras de almacenamiento de los documentos, bajo el control de los usuarios.
    - Está orientado primariamente a dar soporte a la gestión diaria de los documentos para el desarrollo de los procesos de negocio.

- **SGDEA**. Un SGDEA, por el contrario, se caracteriza por lo siguiente:
    - Impide que los documentos de archivo sean modificados.
    - Sólo permite la existencia de una versión final de los documentos.
    - Impide el borrado de los documentos salvo en determinadas circunstancias estrictamente controladas.
    - Incluye controles de conservación y eliminación rigurosos.
    - Facilita una estructura rigurosa de organización de los documentos, mediante el cuadro de clasificación.
    - Está dirigido principalmente a proporcionar un repositorio seguro a los documentos fruto de los procesos de negocio aunque, ocasionalmente, puede dar soporte al trabajo de las oficinas.

Además, un SGDEA debe poder gestionar calendarios de conservación, seleccionar de modo automático expedientes y documentos para llevar a cabo las acciones dictaminadas para su serie documental, así como detectar aquellos documentos que, por sus circunstancias, deban ser objeto de acciones específicas de conservación. Asimismo, debe poder gestionar el acceso a los expedientes y documentos mediante listas y perfiles de usuario, así como disponer de sistemas de seguimiento y control de las acciones que se realicen sobre los documentos y expedientes.

De las características mencionadas anteriormente se desprende que un SGDE se correspondería más con un archivo de oficina, mientras que un SGDEA albergaría documentos y expedientes en sus versiones finales, es decir, en fase de archivo central, intermedio e histórico. Partiendo de la normativa vigente, deben determinarse las condiciones en que debe producirse la transferencia de documentos entre ambos

sistemas.

Sin embargo, en el momento actual se dan algunas peculiaridades que han de tenerse en cuenta:

- No es posible establecer una frontera nítida entre los distintos sistemas de gestión de los documentos existentes en la Generalitat, ya que un mismo sistema alberga documentos de archivo y documentos aún no definitivos.
- Es frecuente que los controles propios de un SGDEA de cara a la integridad y control de acceso a los documentos no los proporcione un sistema de gestión, sino las propias aplicaciones de gestión.
- Los documentos no cumplen en muchas ocasiones los requisitos del ENI, ya que se considera que éstos únicamente deben implementarse en el momento de una transferencia y no mientras permanezcan bajo el control de los órganos gestores.

En consecuencia, se propone que el SGDEA comience en la fase de Archivo Central, momento en que los expedientes y documentos que se transfieran al mismo deberán tener implementados, al menos, los metadatos obligatorios para intercambio del ENI y además los que queden establecidos en el esquema institucional de metadatos de la Generalitat como obligatorios para la transferencia con cambio de responsabilidad de la custodia y la gestión.

Esto no obsta para que determinadas aplicaciones de gestión o SGDE puedan necesitar implementar utilidades de SGDEA (resellado, cambios de formato, etc.), debido a que los expedientes resultantes de los procedimientos que tramitan puedan tener un período de vida activa que haga necesaria la aplicación de políticas de conservación a medio o largo plazo.

Dicho programa de tratamiento se aplicará de manera continua sobre todas las etapas o periodos del ciclo de vida de los documentos y expedientes electrónicos para los que se garantizará su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, permitiendo la protección, recuperación y conservación física y lógica de los documentos y su contexto.

En el futuro, se tenderá en la medida de lo posible al uso de las mismas aplicaciones de gestión documental en el ámbito de la Generalitat y sus organismos dependientes, en función de la que se determine de máxima utilidad para los objetivos pretendidos y de mayor grado de interoperabilidad.

Cuando se precise formalizar contratos con empresas para la externalización de determinados procesos de gestión documental, como podrían ser la digitalización de archivos en papel, la destrucción segura de documentos, etc., se recomienda incluir una cláusula por la que se exija a las empresas adjudicatarias acreditar los niveles de idoneidad técnica establecidos en los estándares que sean de aplicación. En todo caso, se recogerá una cláusula de confidencialidad de obligado cumplimiento para las empresas adjudicatarias.

2.5.1. Captura

La captura del documento electrónico es el proceso que señala su entrada en un sistema de gestión de documentos electrónicos y garantiza su identificación unívoca. En el momento de la captura se establece una relación entre el documento, su productor o creador y el contexto en que se originó. Este propósito se consigue mediante la asignación de los metadatos mínimos obligatorios definidos en la NTI de Documento

Electrónico así como mediante la asignación al documento de un identificador único.

La captura del documento en el sistema de gestión de documentos de la organización incluiría los procesos de registro e incorporación de los documentos en el sistema de gestión de documentos de la organización, y, como acción de especial relevancia, incluiría la asignación de los metadatos y, si procede, la firma del documento por parte de la Generalitat. Esta captura del documento, puede venir precedida por una digitalización, según lo dispuesto en la NTI de Digitalización de Documentos, o por un proceso de conversión de formato del documento, según lo dispuesto en la NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, en caso necesario.

La captura de un documento electrónico, además, y siguiendo esta misma guía de aplicación, se completa con otros procesos y operaciones de gestión de documentos, como la clasificación o su inclusión en un expediente electrónico, tal y como se indica en la NTI de Expediente Electrónico.

Este concepto de captura da por sentado que el proceso tiene lugar en un escenario en el que:

- La organización tiene operativo un SGDE.
- Este SGDE da cobertura a toda la organización.
- La operación de registro es independiente de la captura, ya que puede darse o no.
- Si la operación de registro del documento se da, se produce en el propio seno de la organización que lo va a gestionar mediante su SGDE.

La fecha de captura del documento se corresponderá con la fecha de su ingreso en el sistema de gestión documental (SGDE) empleado en la organización. Esta fecha puede diferir de su fecha de digitalización. También podrá diferir de la fecha de registro administrativo del documento, cuando se verifique el mismo.

El identificador único asignado a los documentos electrónicos capturados seguirá la codificación:

ES_<ÓRGANO>_<AAAA>_<ID_ESPECIFICO>[4]	
<ÓRGANO>	Se codificará según lo establecido en el Directorio Común (DIR3) *Ejemplos:* A10017552 CONSELLERIA DE HACIENDA Y MODELO ECONÓMICO A10017582 SUBSECRETARÍA - CONSELLERIA DE HACIENDA Y MODELO ECONÓMICO A10018001 SUBDIRECCIÓN GENERAL DEL LIBRO, ARCHIVOS Y BIBLIOTECAS
<AAAA>	Año de la fecha de captura del documento
<ID_ESPECIFICO>	Código alfanumérico[5] que identifica de forma única al documento dentro de los generados por la administración responsable, con tamaño máximo de 30 caracteres

4 Según NTI del Documento Electrónico

5 Se recomienda utilizar un código secuencial o un identificador automático generado por el propio programa de tratamiento (SGDE).

Se señalan a continuación aquellos metadatos mínimos obligatorios definidos por la NTI de Documento Electrónico que deben completarse en el momento de la captura del documento, cuyos valores sería difícil o imposible recuperar en fases posteriores de la gestión documental.

Metadato	Asignación en punto de captura de SGDE	Asignación en cualquier momento
Versión NTI	✓	
Identificador	✓	
Órgano	✓	
Fecha de captura	✓	
Origen	✓	
Estado de elaboración	✓	
Nombre del formato	✓	
Tipo documental		✓
Tipo de firma	✓	
Valor CSV[6]	✓	
Definición generación CSV[7]	✓	
Identificador del documento en origen[8]	✓	

Del mismo modo, se cumplimentarán los metadatos mínimos obligatorios de los expedientes electrónicos, en el momento de su creación, ya que con respecto al expediente electrónico no se puede hablar en sentido estricto de fase de captura. Tales metadatos, que aparecen relacionados en la NTI de Expediente Electrónico son los siguientes:

Metadato	Asignación en momento de creación	Asignación en cualquier momento
Versión NTI	✓	
Identificador	✓	
Órgano	✓	
Fecha apertura expediente	✓	
Clasificación	✓	
Estado		✓

6 Estos metadatos sólo aparecen si el "Tipo de Firma" es CSV.
7 Ídem a nota anterior.
8 Este metadato sólo aparece si el "Estado de elaboración" es "Copia electrónica auténtica con cambio de formato" o "Copia electrónica parcial auténtica".

Interesado		✓
Tipo de firma	✓	
Valor CSV[9]	✓	
Definición generación CSV[10]	✓	

2.5.2. Registro

A los efectos de la presente Política de Gestión de Documentos Electrónicos, se entiende por Registro el proceso de control mediante la correspondiente inscripción registral de los documentos generados o recibidos por los órganos administrativos de la Generalitat.

El registro y tramitación de los documentos electrónicos en la Generalitat se realizarán conforme al Decreto 220/2014, de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.

En concreto, el registro electrónico se regula en el título IV de la citada norma, especificando en el apartado 6 del artículo 50 que *"todos los documentos deberán estar realizados en formatos o aplicaciones informáticas definidas por el Esquema Nacional de Interoperabilidad, en las normas técnicas que dicte la Generalitat para adaptarse a estos"*.

Los trámites y modelos susceptibles de registro electrónico estarán a disposición de la ciudadanía en la Sede Electrónica de la Generalitat (https://sede.gva.es).

Cuando la presentación de la documentación sea en una de las oficinas de asistencia en materia de registros presenciales de la Generalitat, la misma se regirá por lo establecido en el Decreto 191/2014, de 14 de noviembre, del Consell, por el que se regula la atención a la ciudadanía, el registro de entrada y salida de escritos y la ordenación de las oficinas de registro en la Administración de la Generalitat. El procedimiento a seguir se detalla en el manual de instrucciones de obligado cumplimiento para todas las oficinas de asistencia en materia de registros de la Generalitat, aprobado por Resolución de 5 de mayo de 2015 por el órgano competente, como desarrollo del Decreto 191/2014.

La relación actualizada de las oficinas de asistencia en materia de registros, así como sus datos de ubicación y horario estarán a disposición de la ciudadanía en la guía PROP electrónica del portal de la Generalitat (www.gva.es).

2.5.2.1. Documentación en soporte no electrónico

Toda documentación en soporte papel o en otro soporte susceptible de digitalización que se presente en las oficinas de asistencia en materia de registros deberá producir un asiento registral y la copia a devolver al interesado deberá llevar el correspondiente acuse de recibo que acredite la presentación de la misma, salvo que no pudiera obtenerse en el momento, en cuyo caso se deberá estampar en dicha copia un sello de registro en el que figure la fecha de entrada de la documentación.

9 Estos metadatos sólo aparecen si el "Tipo de Firma" es CSV.

10 Ídem a nota anterior.

Todos los documentos en soporte papel o en otro soporte susceptible de digitalización presentados en las oficinas de asistencia en materia de registros deberán ser digitalizados con el fin de obtener una copia electrónica auténtica, de acuerdo con lo previsto en los artículos 16 y 27 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en el artículo 60 del Decreto 220/2014 de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana. Para ello se dotará a dichas oficinas con los medios técnicos necesarios para la digitalización.

Se exceptúan de lo previsto en el párrafo anterior los siguientes supuestos:

- Los sobres cerrados presentados en las oficinas de asistencia en materia de registros en el marco de licitaciones públicas, ya sean enajenaciones forzosas en procedimientos de recaudación o en procedimientos de contratación pública, que no se abrirán ni escanearán.
- Otras excepciones específicas que puedan existir.

En este caso, los documentos deberán ser remitidos inmediatamente a sus destinatarios, en sobre cerrado.

El procedimiento de digitalización se llevará a cabo en cualquier caso cumpliendo las especificaciones de las Normas Técnicas de Interoperabilidad de Digitalización y de Documento Electrónico y, en particular, el protocolo de digitalización incluido en esta política.

2.5.2.2. Metainformación del asiento registral y de los documentos anexos

La información descriptiva referente al asiento registral que debe ser introducida de modo automático o manual en el proceso de registro será la que se contempla en el apartado IV.2 *Estructura y contenido del mensaje de datos de intercambio*, de la NTI de Modelo de Datos de Intercambio de asientos registrales entre unidades SICRES 3.0.

En caso de incluirse como anexos documentos digitalizados, conforme a la NTI de Digitalización de Documentos, la metainformación referente a estos últimos, según apartado III.1.b de la mencionada norma, será la definida como mínima obligatoria en el Anexo I de la NTI de Documento Electrónico. Podrán asociarse, además, de forma complementaria, metadatos relacionados con el proceso de digitalización que reflejen las características técnicas de la imagen electrónica capturada, así como otros metadatos propios del trámite o procedimiento administrativo al que pertenezca el documento.

2.5.3. Clasificación

2.5.3.1. Criterios de formación de expedientes electrónicos y agrupaciones de documentos.

En el Anexo del ENI (Esquema Nacional de Interoperabilidad) se define un documento electrónico como *"información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"*. El documento electrónico constituye la base para conformar tanto expedientes como agrupaciones de documentos electrónicos.

Siempre que sea posible, dichos expedientes y agrupaciones estarán constituidos exclusivamente por documentos electrónicos, excepto cuando por la naturaleza del procedimiento fuera necesario mantener expedientes híbridos que contengan documentación en soporte no electrónico.

Para evitar la generación de expedientes híbridos, se digitalizarán y se obtendrán copias electrónicas auténticas de los documentos en papel, de modo que serán estas copias las que se incorporen al expediente electrónico.

Los expedientes electrónicos y agregaciones de documentos electrónicos producidos por la entidad atenderán a los siguientes criterios de formación y patrones:

- Expedientes administrativos electrónicos:
  - La NTI de Expediente Electrónico establece la estructura y el formato del expediente electrónico, así como las especificaciones de los servicios de remisión y puesta a disposición. Por su parte, el Decreto 220/2014, de administración electrónica de la Generalitat, en su art. 65, señala que *"estará formado por el conjunto de documentos administrativos electrónicos correspondientes a un procedimiento* administrativo".
  - En el expediente electrónico se integran aquellos documentos, administrativos o no, que deban formar parte del mismo por ser el resultado de las actuaciones de la Administración encaminadas a la resolución administrativa de un asunto. No se integrarán en el expediente las versiones de documentos salvo que deban figurar por razón de su normativa específica, en cuyo caso deberán firmarse electrónicamente.
  - En el caso de documentos con anexos, se tratarán, a efectos de validación, como un único documento, o como documentos independientes, vinculados entre sí.
  - Una vez cerrado, el expediente electrónico quedará foliado mediante un índice electrónico en el que se relacionarán todos los documentos que lo componen. Dicho índice será firmado por la Administración, órgano o entidad actuante, que garantiza así la integridad del expediente
  - Según el artículo 57 del Decreto 220/2014 y el Apartado IV de la NTI, Norma Técnica de Interoperabilidad de documento electrónico, los documentos administrativos electrónicos, y aquellos susceptibles de formar parte de un expediente, tendrán siempre asociada al menos una firma electrónica de acuerdo con la normativa aplicable.
  - El índice electrónico de los expedientes objeto de intercambio reflejará al menos:
    - Fecha de generación del índice (ya que refleja el estado del expediente en un determinado momento).
    - Para cada documento electrónico: su identificador, su huella digital, la función resumen y, opcionalmente, la fecha de incorporación al expediente y el orden del documento en el expediente.
    - La fecha de incorporación al expediente es opcional porque:
      - En algunos casos se desconoce.
      - En la mayoría, cobra más importancia la fecha de firma o publicación del documento, momento en que empieza el plazo legal.
    - El orden del documento en el expediente será un tipo cadena de caracteres, no necesariamente un índice entero.

- Si es el caso, los documentos podrán disponerse en carpetas y expedientes electrónicos anidados.
- Firma del índice electrónico por la Administración, órgano o entidad actuante, mediante los sistemas de firma previstos en el artículo 42, Sistemas de firma para la actuación administrativa automatizada de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ó artículo 43, Firma electrónica del personal al servicio de las Administraciones Públicas. Los órganos administrativos podrán añadir elementos complementarios a la estructura del índice, siempre que ello no afecte a la interoperabilidad del expediente, y en todo caso estará de acuerdo con el art. 31, Identificación y autenticación del empleado público, y los artículos 79 y 80, de Acreditación mediante códigos seguros de verificación de documentos y Acreditación mediante códigos seguros de verificación de documentos, respectivamente, del Decreto 220/2014, de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.

Dicho decreto, en su art. 65.2, establece las reglas que se han de seguir en su formación:

a) Los expedientes electrónicos dispondrán de un código único e inalterable.

b) Los expedientes electrónicos deberán tener asociados los metadatos necesarios para su correcta tramitación y conservación.

c) El foliado de los expedientes electrónicos se llevará a cabo mediante un índice firmado electrónicamente.

d) Los expedientes electrónicos pueden incluir, asimismo, otros expedientes electrónicos si así lo requiere el procedimiento.

- Agrupaciones documentales:

De acuerdo con lo dispuesto en el apartado II.2 de la NTI de Expediente Electrónico, entendemos por agrupaciones documentales conjuntos de documentos electrónicos que, habiendo sido creados al margen de un procedimiento reglado, se hubiesen formado mediante agregación, como resultado de una secuencia de actuaciones coherentes que conducen a un resultado específico.

Dado que no son consecuencia de un procedimiento, podrán carecer de valor jurídico y, por ello, su formalización como documentos administrativos electrónicos, con contenido, firma y metadatos, seguramente será excepcional.

No obstante, su tratamiento a efectos de gestión documental deberá ser análogo al de los expedientes sujetos a un procedimiento, lo que exigirá que reúnan las siguientes características:

- Sólo deben integrarse en la agrupación documentos finales, se deben excluir los borradores.
- Los documentos deben estar dotados de un identificador único.
- Todos los documentos deben estar fechados.
- La agrupación documental debe considerarse cerrada en un momento determinado, sin admitir nuevos documentos.
- Los documentos deben reseñarse también en un índice electrónico.

- Aunque no tengan firma, se debe obtener el *hash* o función resumen del documento, lo que garantizaría, al menos, su integridad.
- El índice electrónico recopilará el identificador, la huella, la fecha de los documentos y el orden dentro de la agrupación, si es relevante.
- En la medida de lo posible, se asignarán metadatos análogos a los obligatorios de expediente electrónico.

- Documentos simples:

  También es posible aplicar la clasificación documental a documentos simples, que no estén integrados en un expediente electrónico ni en una agrupación documental. Su tratamiento a efectos de gestión documental deberá reunir las características siguientes:

  - Sólo se deben almacenar documentos finales, excluyendo los de otra naturaleza, como los borradores de documento.
  - Los documentos deben estar dotados de un identificador único.
  - Todos los documentos deben estar fechados.
  - Todos los documentos deben estar firmados electrónicamente
  - En el caso de documentos con anexos, se tratan, a efectos de validación, como un único documento, o como documentos independientes, vinculados entre sí.
  - El documento debe tener asignados los metadatos correspondientes según la NTI relativa al documento electrónico.

2.5.3.2. Cuadro de clasificación funcional

El cuadro de clasificación funcional aparece claramente definido en:

- El artículo 21 del ENI establece que:

  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:*

  …

  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.

- Por su parte, el artículo 10.1, del Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, al enumerar las funciones de los archivos centrales, establece entre ellas:

  "2.º Llevar a cabo el proceso de identificación de series y elaborar el cuadro de clasificación."

- La necesidad de contar con un cuadro de clasificación funcional se desprende asimismo de lo

dispuesto en la NTI de Política de Gestión de Documentos Electrónicos, al contemplar en su apartado VI.3, la Clasificación de los documentos como uno de los procesos de gestión de los mismos:

Clasificación de documentos, que incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la NTI de Expediente Electrónico, así como la clasificación funcional de acuerdo con el cuadro de clasificación de la organización.

- La Norma UNE-ISO 15489, por su parte, al tratar el proceso de gestión de Clasificación en su apartado 9.5.1., dice:

  "La Clasificación de las actividades de la organización representa una poderosa herramienta para el desarrollo de las mismas y para muchos procesos de gestión, como:

  a) el establecimiento de vínculos entre documentos individuales que reunidos proporcionan una representación continua de la actividad;

  b) la garantía de que los documentos se denominan de modo coherente a lo largo del tiempo;

  c) la ayuda a la recuperación de todos los documentos relacionados con una función o una actividad concreta;

  d) la definición de niveles de seguridad y acceso adecuados para conjuntos de documentos;

  e) la atribución de permisos de acceso a los usuarios para acceder a determinados grupos de documentos u operar en los mismos;

  f) la distribución de la responsabilidad de la gestión de determinados grupos de documentos;

  g) la distribución de los documentos para la realización de las tareas oportunas; y

  h) el establecimiento de plazos y medidas de conservación y disposición apropiados."

La clasificación de los documentos y expedientes atenderá a los pertinentes cuadros de clasificación, desarrollados específicamente por los departamentos de la Generalitat y otros entes incluidos en el ámbito de aplicación de esta Política. Dichos cuadros de clasificación se incorporarán como anexo a este documento conformando un cuadro único para toda la Generalitat, el cuál será actualizado sistemáticamente siempre que haya alguna modificación normativa, estructural o funcional que le afecte, sin necesidad de modificar el documento de PGDE-GV.

El cuadro actual de clasificación elaborado para la Generalitat es de naturaleza orgánico-funcional, considerando tanto el órgano o unidad que origina el documento como la finalidad del mismo.

El cuadro de clasificación funcional se realizará en el plazo máximo de un año desde la aprobación de este documento de gestión de política documental. La alta dirección de la organización impulsará la sensibilización de las diferentes oficinas que producen y gestionan los documentos y expedientes con el fin de que proporcionen los datos necesarios para poder materializar el citado cuadro de clasificación funcional.

2.5.3.3. Repertorio de series documentales

En tanto se apruebe el cuadro de clasificación, para la puesta en marcha del sistema de gestión de documentos, se elaborará un repertorio de series documentales de la Generalitat, que se incorporará como anexo a este documento desde el mismo momento de su aprobación. El anexo del repertorio de series será

actualizado periódicamente, sin necesidad de que dicha actualización implique modificación de este documento de Política de Gestión de Documentos Electrónicos.

2.5.3.4. Situación transitoria hasta la elaboración del cuadro de clasificación funcional

Dada la necesidad de contar con algún tipo de clasificación que permita poner en marcha el sistema de gestión de documentos, ésta se realizará sobre la base del Repertorio de Series, identificadas, en su caso, por las que hay establecidas por el Archivo Histórico *de la Comunitat Valenciana*, algunos cuadros de clasificación elaborados por los departamentos de la Generalitat y el catálogo de procedimientos. Asimismo, se incluirá el repertorio de series valoradas por la JCDA.

Tanto las series identificadas como el posterior Cuadro de Clasificación figurarán en anexos a la PGDE-GV, de manera que puedan ser modificados sin alterar el contenido del documento.

2.5.4. Descripción

La descripción de los documentos y expedientes electrónicos permitirá la recuperación de los mismos y su contexto, y atenderá a la aplicación del esquema institucional de metadatos.

2.5.4.1. Orientaciones y requisitos tenidos en cuenta para la construcción de un esquema de metadatos

De acuerdo con el apartado VII de la NTI de Política de Gestión de Documentos electrónicos:

- *Las organizaciones garantizarán la disponibilidad e integridad de los metadatos de sus documentos electrónicos, manteniendo de manera permanente las relaciones entre cada documento y sus metadatos.*
- *La implementación de los metadatos de gestión de documentos electrónicos para su tratamiento y gestión a nivel interno será diseñada por cada organización en base a sus necesidades, criterios y normativa específica.*
- *Los metadatos de gestión de documentos electrónicos se articularán en esquemas de metadatos que responderán a las particularidades y necesidades específicas de gestión de cada organización.*
- *El Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), disponible en el Centro de Interoperabilidad Semántica, que 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 electrónicos, podrá ser utilizado como referencia para la adecuación a los requisitos de interoperabilidad en materia de gestión documental.*

En concordancia con las directrices de la ISO 23081, para una organización es más eficaz y sencillo adoptar un esquema normalizado de metadatos, como el e-EMGDE, ya existente, que esté bien diseñado, y cuente con apoyo institucional, que construir un esquema específico. La construcción de un esquema nuevo implicaría la necesidad de gestionarlo y mantenerlo durante el tiempo de vida de los documentos, incluyendo la actualización del esquema y la verificación de la compatibilidad en el pasado y en el futuro, la aparición de metadatos sobre el esquema de metadatos, su catalogación y el resto de la infraestructura necesaria para mantener la implementación, etc.

Por los motivos expuestos, y dado que el esquema de metadatos recomendado por el ENI es e-EMGDE, partiremos del mismo para establecer un esquema institucional de metadatos para la Generalitat, e-EMGDE-GV, que permita cumplir simultáneamente dos objetivos:

- Soportar todas las transacciones que tienen lugar en los procesos de gestión documental identificados en la NTI de Política de Gestión de Documentos Electrónicos.
- Permitir a los diferentes organismos que lleven a cabo la adecuación al ENI con un esfuerzo de desarrollo moderado.

Siempre que sea posible, se deberá evitar introducir un elemento nuevo, dado que reduce la interoperabilidad. En consecuencia, si fuera necesario introducir algún cambio, se limitarían a introducir:

- Mejoras específicas, es decir, subelementos adicionales.
- Esquemas codificados específicos, por ejemplo listas controladas de términos, reglas sobre como introducir nombres, fechas, etc.

El anexo II recoge el perfil de aplicación de la Generalitat, con una selección de los metadatos considerados más importantes y de uso más generalizado. No obstante, se podrán adoptar los metadatos que se consideren necesarios o aconsejables para la gestión y, en este sentido, todo el e-EMGDE-GV se considera metadatos recomendados.

Aunque el e-EMGDE-GV se ha pensado en un inicio como un modelo multientidad, el desarrollo inicial se limitará a un modelo monoentidad. Con el fin de optimizar los recursos que proporcionaría el modelo relacional, se avanzará progresivamente y en colaboración con otras Administraciones para estructurar el Modelo de Metadatos Multientidad y fortalecer el contexto de producción de los documentos y expedientes electrónicos, a los que se adhiere la Generalitat.

METADATOS OBLIGATORIOS NTI DE DOCUMENTO Y EXPEDIENTE ELECTRÓNICO
e-EMGDE2 - IDENTIFICADOR
e-EMGDE2.1 - SECUENCIA DE IDENTIFICADOR
e-EMGDE4 - FECHAS
e-EMGDE4.1 - FECHA INICIO[11]
e-EMGDE14 - CARACTERÍSTICAS TÉCNICAS
e-EMGDE14.1 - FORMATO
e-EMGDE14.1.1 - NOMBRE DEL FORMATO
e-EMGDE14.1.2 - EXTENSIÓN DEL FICHERO
e-EMGDE17 - FIRMA
e-EMGDE17.1 - TIPO DE FIRMA
e-EMGDE17.1.1 - FORMATO DE FIRMA
e-EMGDE17.3 – VALOR DEL CSV *(Si tipo de firma es TF01 (CSV))*
e-EMGDE17.4 - DEFINICIÓN GENERACIÓN CSV *(Si tipo de firma es TF01 (CSV))*
e-EMGDE18 - TIPO DOCUMENTAL
e-EMGDE20 - ESTADO DE ELABORACIÓN
e-EMGDE22 – CLASIFICACIÓN *(Para Expediente)*
e-EMGDE22.1 - CÓDIGO DE CLASIFICACIÓN
e-EMGDE23 - VERSIÓN NTI
e-EMGDE24 - ÓRGANO
e-EMGDE25 - ORIGEN DEL DOCUMENTO
e-EMGDE26 - IDENTIFICADOR DEL DOCUMENTO ORIGEN *(Si estado de elaboración es EE02, EE03, EE04)*
e-EMGDE27 - ESTADO DEL EXPEDIENTE *(Para Expediente)*
e-EMGDE28 – INTERESADO

11 Hace referencia a la Fecha de Captura de las NTI de Documento Electrónico y a la Fecha de Apertura de Expedientes de las NTI de Expediente Electrónico

OTROS METADATOS OBLIGATORIOS DE DOCUMENTO Y EXPEDIENTE ELECTRÓNICO
e-EMGDE3 – NOMBRE e-EMGDE3.1 – NOMBRE NATURAL **e-EMGDE17 - FIRMA** e-EMGDE17.1 - TIPO DE FIRMA e-EMGDE17.1.2 - PERFIL DE FIRMA *(Si tipo de firma es distinto de TF01 (CSV))* e-EMGDE17.2 – ROL DE FIRMA *(Si se utiliza más de una firma y cada una de ellas tiene una función diferente)*

METADATOS COMPLEMENTARIOS MÍNIMOS NECESARIOS PARA LA TRANSFERENCIA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS ENTRE REPOSITORIOS CON CAMBIO DE CUSTODIA

e-EMGDE1 – CATEGORÍA

e-EMGDE4.2 - FECHA FIN

e-EMGDE8 - SEGURIDAD

- e-EMGDE8.4 - SENSIBILIDAD DATOS DE CARÁCTER PERSONAL
- e-EMGDE8.5 – CLASIFICACIÓN ENS
- e-EMGDE8.6 - NIVEL DE CONFIDENCIALIDAD DE LA INFORMACIÓN

e-EMGDE9 - DERECHOS DE ACCESO, USO Y REUTILIZACIÓN

- e-EMGDE9.1 - TIPO DE ACCESO
- e-EMGDE9.2 - CÓDIGO DE LA CAUSA DE LIMITACIÓN
- e-EMGDE9.3 - CAUSA LEGAL/NORMATIVA DE LIMITACIÓN
- e-EMGDE9.4 - CONDICIONES DE REUTILIZACIÓN

e-EMGDE13 – CALIFICACIÓN

- e-EMGDE13.1 - VALORACIÓN
  - e-EMGDE13.1.1 - VALOR PRIMARIO
    - e-EMGDE13.1.1.1. TIPO DE VALOR
    - e-EMGDE13.1.1.2. PLAZO
  - e-EMGDE13.1.2 - VALOR SECUNDARIO
- e-EMGDE13.2 - DICTAMEN
  - e-EMGDE13.2.1 - TIPO DE DICTAMEN
  - e-EMGDE13.2.2 - ACCIÓN DICTAMINADA
  - e-EMGDE13.2.3 - PLAZO DE EJECUCIÓN DE LA ACCIÓN DICTAMINADA
- e-EMGDE13.3 - TRANSFERENCIA
  - e-EMGDE13.3.1 - FASE DE ARCHIVO
  - e-EMGDE13.3.2 - PLAZO DE TRANSFERENCIA

METADATOS COMPLEMENTARIOS MÍNIMOS NECESARIOS PARA LA TRANSFERENCIA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS ENTRE REPOSITORIOS CON CAMBIO DE CUSTODIA
e-EMGDE13.4 - DOCUMENTO ESENCIAL **e-EMGDE22 - CLASIFICACIÓN** e-EMGDE22.2 - DENOMINACIÓN DE CLASE e-EMGDE22.3 - TIPO DE CLASIFICACIÓN (SIA/FUNCIONAL)

METADATOS COMPLEMENTARIOS RECOMENDADOS PARA LA GESTIÓN ÓPTIMA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS
e-EMGDE29 – ASIENTO REGISTRAL e-EMGDE29.1 – TIPO DE ASIENTO REGISTRAL e-EMGDE29.2 – CÓDIGO DE LA OFICINA DE REGISTRO e-EMGDE29.3 – FECHA DEL ASIENTO REGISTRAL e-EMGDE29.4 – NÚMERO DE ASIENTO REGISTRAL **e-EMGDE3 – NOMBRE** e-EMGDE3.2 – NOMBRE DEL FICHERO **e-EMGDE5 – DESCRIPCIÓN** **e-EMGDE11 – IDIOMA** **e-EMGDE12 – PUNTOS DE ACCESO** e-EMGDE12.1 – TÉRMINO PUNTO DE ACCESO e-EMGDE12.2 – ID PUNTO DE ACCESO e-EMGDE12.3 – ESQUEMA PUNTO DE ACCESO **e-EMGDE14 – CARACTERÍSTICAS TÉCNICAS** e-EMGDE14.2 – VERSIÓN DE FORMATO e-EMGDE14.3 – RESOLUCIÓN e-EMGDE14.4 – TAMAÑO e-EMGDE14.4.2 – TAMAÑO LÓGICO e-EMGDE14.5 – PROFUNDIDAD DE COLOR **e-EMGDE15 – UBICACIÓN** e-EMGDE15.1 - SOPORTE e-EMGDE15.2 - LOCALIZACIÓN **e-EMGDE16 – VERIFICACIÓN DE INTEGRIDAD** e-EMGDE16.1 - ALGORITMO

METADATOS COMPLEMENTARIOS RECOMENDADOS PARA LA GESTIÓN ÓPTIMA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS

e-EMGDE16.2 - VALOR

e-EMGDE17 – FIRMA

e-EMGDE17.5 – FIRMANTE

e-EMGDE17.5.1 – NOMBRE Y APELLIDOS O RAZÓN SOCIAL

e-EMGDE17.5.2 – NÚMERO DE IDENTIFICACIÓN DEL/DE LOS FIRMANTE/S

e-EMGDE17.5.3 – EN CALIDAD DE

e-EMGDE17.5.4 – NIVEL DE FIRMA

e-EMGDE17.5.5 – INFORMACIÓN ADICIONAL

e-EMGDE21 – TRAZABILIDAD

e-EMGDE21.1 – ACCIÓN

e-EMGDE21.1.1 – DESCRIPCIÓN DE LA ACCIÓN

e-EMGDE21.1.2 – FECHA DE LA ACCIÓN

e-EMGDE21.1.3 – ENTIDAD DE LA ACCIÓN

e-EMGDE21.2 – MOTIVO REGLADO

e-EMGDE21.3 – USUARIO DE LA ACCIÓN

e-EMGDE21.4 – DESCRIPCIÓN

e-EMGDE21.5 – MODIFICACIÓN DE LOS METADATOS

e-EMGDE21.6 – HISTORIA DEL CAMBIO

e-EMGDE21.6.1 – NOMBRE DEL ELEMENTO

e-EMGDE21.6.2 – VALOR ANTERIOR

Para la descripción de los documentos y expedientes se tendrán en cuenta recursos como los siguientes:

- Tesauro.
- Vocabulario de lenguaje controlado.
- Índices de materias.
- Otros.

Se tendrá en cuenta, en el futuro, el desarrollo de recursos de este tipo que ayuden en la gestión documental y se añadirán como anexo al documento, de manera que su actualización o alteración no supondrá modificación del documento de Política de Gestión de Documentos Electrónicos. Mientras tanto, podrán usarse las herramientas existentes en las distintas unidades, si bien hay que tener en cuenta que al no estar normalizados, estos recursos específicos de las unidades carecen de utilidad en las transferencias.

2.5.5. Acceso y trazabilidad

El acceso a los documentos y expedientes electrónicos, sus índices y metadatos asociados deben ser sometidos a un control de acceso en función de los datos contenidos en los documentos almacenados. El SGDE/SGDEA debe asegurar la identificación de los usuarios y el control de acceso, sus permisos y responsabilidades, así como el cumplimiento de las garantías previstas en la legislación relativa a restricciones en materia de acceso. Además, debe asegurar que quede traza de todas las acciones que se realicen sobre cada uno de los documentos y expedientes electrónicos y sus metadatos asociados, siguiendo lo establecido en la política de seguridad adoptada por parte de la organización.

El sistema debe ser capaz de resistir, con un determinado nivel de confianza, los accidentes y las acciones ilícitas o mal intencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o trasmitidos y de los servicios ofrecidos, o a través de los cuales se realiza el acceso.

Se deberán establecer los criterios que determinen los privilegios y las restricciones de acceso a las distintas entidades relacionadas con los documentos, de manera que se garantice la protección lógica y física de las mismas.

Desde el punto de vista operativo, la implementación de la seguridad deberá realizarse estableciendo los correspondientes perfiles, roles y derechos de los usuarios en las aplicaciones de gestión documental.

Para la definición de los sujetos de acceso se deberá delimitar los tipos de usuarios que tendrán los mismos permisos o roles. Dependiendo de si el alcance de la implementación incluye alguna o todas las fases del ciclo de vida de los expedientes, tramitación, vigencia o conservación permanente, se deberán crear como mínimo los siguientes roles de usuario para cada fase:

- Tramitadores. Crean, capturan, modifican y validan documentos dentro de los expedientes de la serie.
- Responsables de serie. Crean expedientes, los modifican y los cierran.

- Supervisores. Consultan los expedientes y documentos, pero no pueden modificarlos, aunque los expedientes no estén cerrados.
- Usuarios de consulta. Consultan los expedientes y los documentos solo cuando los expedientes están cerrados.
- Gestores documentales. Crean la estructura del repositorio y supervisan su funcionamiento.

De este modo, para cada serie documental, el resultado del diseño deberá identificar y definir:

- Los agentes que intervienen en la gestión del ciclo de vida de los documentos de la serie y los canales de comunicación a través de los cuales llegarán los documentos, siguiendo el Modelo de Información que se haya definido.
- Las relaciones de la serie con otras series del Esquema de Clasificación Funcional.
- Cómo generar y preservar todo documento del expediente.
- Las políticas de seguridad y acceso a nivel de expediente y documento.

2.5.5.1. Requisitos de Seguridad y Acceso

La seguridad de la información es un proceso transversal que tiene como objetivo final la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Los requisitos de seguridad y acceso que hay que tener en cuenta afectan:

- A los propios documentos donde habrá que implementar metadatos que informen sobre las restricciones de acceso incluyendo, además, mecanismos que permitan ofrecer un acceso parcial a los mismos, ocultando los datos y contenidos objeto de protección.
- Al SGDE/SGDEA en su conjunto con el fin de evitar el acceso a usuarios no autorizados a los documentos y expedientes, según lo establecido en la norma ISO 15489.

Las Tablas de Acceso y Seguridad son el instrumento formal que contempla la norma ISO 15489, en su apartado 4.2.5, para la identificación de los derechos de acceso y el régimen de restricciones aplicables a los documentos. Se conforman como una clasificación de categorías de documentos en función de sus restricciones de acceso y condiciones de seguridad.

Más allá de las especificaciones de la ISO mencionadas, será también necesario ajustarse al marco legal y competencial de la Generalitat y, para cada serie documental, utilizar las Tablas de Valoración Documental con el fin de determinar el régimen aplicable al acceso, así como los criterios sobre la aplicación de la normativa competencial que rige el acceso a los documentos y su disposición (Ley 3/2005, Ley de Archivos).

El régimen general de acceso a los documentos y expedientes deberá quedar establecido para cada una de las series documentales. Deberán elaborarse las Tablas de Valoración Documental, incorporando las restricciones legales, de confidencialidad y de protección de datos personales.

De acuerdo con la Política de Seguridad de la Organización, cada uno de los documentos almacenados en el SGDE/SGDEA tendrá asignado un nivel de acceso. Este nivel de acceso determinará el grado de confidencialidad de la información que contiene y, como consecuencia, qué personas están autorizadas para consultar y modificar el documento.

Previamente, y con el fin de definir dichos niveles y posteriormente poder establecer las bases para elaborar tablas de acceso y seguridad, es recomendable:

- Recopilar las fuentes jurídicas y políticas que han de gobernar el acceso y la seguridad de la información presente en los documentos de la organización
- Definir las categorías de información susceptibles de protección y los plazos de acceso a cada una de ellas a tenor de las fuentes recopiladas, así como los requisitos de seguridad de la información que afectan a la organización
- Identificar las categorías de información susceptibles de protección que contiene cada serie documental y asignar a cada una de ellas los controles de acceso y uso acordes al nivel de seguridad correspondiente a dichas categorías
- Aprobar la tabla de acceso y seguridad y plasmar sus requisitos en las herramientas del sistema.

2.5.5.2. Requisitos de acceso a la información contenida en la entidad Documento

2.5.5.2.1. Categorías de acceso

Según el elemento 9.1 del e-EMGDE, Tipos de acceso, las categorías de acceso existentes son: “Libre acceso” y “Acceso restringido”.

Además de las anteriores, se debería contemplar una nueva categoría, “Parcialmente restringido”, aunque dicho valor no figure como tal en el elemento mencionado. Su inclusión responde a la necesidad de reflejar aquellos casos en los que un expediente de libre acceso puede contener uno o más documentos de acceso restringido. Por lo tanto, la categoría tipo de acceso se definirá, con carácter general, al nivel más bajo posible: el de documento simple, tal y como se refleja en las categorías del e-EMGDE para la entidad Documento.

2.5.5.2.1.1. Libre acceso

Será de aplicación a la citada entidad el elemento 9.1 del e-EMGDE, elemento obligatorio para la información de libre acceso y particularmente relevante cuando la información contenida esté sujeta a un régimen de especial publicidad. Se debe incluir información sobre los contenidos afectados y la referencia normativa correspondiente, especialmente a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

En concreto, se utilizará el elemento 9.4 del e-EMGDE cuando la información contenida sea objeto de transparencia activa o reutilización.

2.5.5.2.1.2. Acceso restringido

La inclusión de los metadatos relativos a acceso es necesaria para todos los documentos inscritos en esta categoría.

Para conseguir un buen rendimiento a la hora de acceder a los documentos es altamente recomendable que, aunque la tecnología permita individualizar el acceso para cada documento, los objetos posibles de acceso se determinen en alguno de los niveles de agrupación de los documentos. Hay que tener presente que los documentos incluidos en estas agrupaciones heredan el mismo tipo de acceso que el nivel superior.

La implementación recomendada es la configuración del acceso a nivel de serie documental. Los expedientes que dentro de una serie requieran un acceso particular más estricto pueden ser tratados como excepciones a la regla general.

2.5.5.2.1.2.1. Contenidos susceptibles de protección

Es necesario incluir información sobre los contenidos susceptibles de protección y la referencia normativa correspondiente. Para ello, tal y como se definen en la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno y excluyendo la información con datos de carácter personal, se puede utilizar para codificar los contenidos afectados el esquema de valores definido para el metadato e-EMGDE 9.2, Código de la causa de limitación, incluido en la siguiente tabla:

Cód.	**Código y contenidos de información con acceso restringido**	**Art. LTAIBG**
A	Seguridad nacional	14.1.a
B	Defensa	14.1.b
C	Relaciones exteriores	14.1.c
D	Seguridad pública	14.1.d
E	Prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios	14.1.e
F	Igualdad de las partes en los procesos judiciales y tutela judicial efectiva	14.1.f
G	Funciones administrativas de vigilancia, inspección y control	14.1.g
H	Intereses económicos y comerciales	14.1.h
I	Política económica y monetaria	14.1.i
J	Secreto profesional. Propiedad intelectual e industrial	14.1.j
K	Garantía de la confidencialidad o secreto requerido en procesos de toma de decisión	14.1.k
L	Protección del medio ambiente	14.1.l
M	Otros intereses públicos susceptibles de protección	-
N	Otros intereses privados susceptibles de protección	-

El e-EMGDE podrá recoger valores específicos para la información especialmente reservada, que podrán ser aplicados sobre la tabla anteriormente mencionada.

Para la entidad documento se aplicarán los elementos 9.2 Código de la causa de limitación y 9.3 Causa legal/normativa de limitación del e-EMGDE .

2.5.5.2.1.2.2. Acceso a la información afectada o regulada por normativa específica

En aquellos casos en que las materias tratadas en la serie documental tengan previsto un régimen jurídico específico de acceso a la información, se debe especificar la norma reguladora, tal y como define el elemento e-EMGDE 9.3 Causa legal/normativa de limitación. La tabla que se incluye a continuación recopila un conjunto de valores que se pueden utilizar como referencia, ya que, de conformidad con el segundo apartado de la Disposición adicional primera de la LTAIBG, se regirán por su normativa específica, y por dicha Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.

Régimen	Normativa reguladora
Información ambiental	Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente. Decreto 97/2010, de 11 de junio, del Consell, por el que se regula el ejercicio del derecho de acceso a la información ambiental y de participación pública en materia de medio ambiente de la Comunitat Valenciana
Información catastral	Ley del Catastro Inmobiliario (texto refundido aprobado por Real Decreto Legislativo 1/2004, de 5 de marzo).
Secreto censal	Ley Orgánica 5/1985, de 19 junio, del Régimen Electoral General.
Secreto fiscal o tributario	Ley 58/2003, de 17 de diciembre, General Tributaria.
Secreto estadístico	Ley 12/1989, de 9 de mayo, de la función estadística pública.
Secreto sanitario	Ley 14/1986, de 25 de abril, General de Sanidad. Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
Materias clasificadas	Ley 9/1968, de 5 de abril, sobre secretos oficiales.
Datos de Carácter Personal	Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la LOPD.
Intimidad y honor	Ley Orgánica 1/1982, de 5 de mayo sobre protección civil del derecho al honor, intimidad personal y familiar y a la propia imagen.

2.5.5.2.1.2.3. Protección de datos de carácter personal

Cuando un documento contenga datos de carácter personal protegidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD, que no tengan la

consideración de “fuentes accesibles al público”, tal y como se establece en el artículo 11, deberá tener asignado un nivel de sensibilidad de datos de carácter personal.

Los niveles de sensibilidad en la clasificación del documento según la LOPD se recogen en la siguiente tabla:

	Datos de carácter personal	**Disposición**
DP1	Datos especialmente protegidos/sensibles/núcleo duro	15.1 LTABG/ LOPD
DP2	Otros datos de carácter personal susceptibles de protección	15.3 LTABG/LOPD
DP3	Otros datos de carácter personal	LOPD

Para asociar a cada documento el nivel que corresponda, se utilizará el metadato e-EMGDE 8.4 Sensibilidad de datos de carácter personal, cuyos valores se recogen en la tabla que se muestra a continuación, en consonancia con la notación propia de la LOPD, el apéndice 12 del e-EMGDE Clasificación de sensibilidad y el metadato del e-EMGDE 8.6 Nivel de confidencialidad de la información.

Nivel	Datos de carácter personal
Alto	Datos especialmente protegidos/sensibles/núcleo duro
Medio	Otros datos de carácter personal susceptibles de protección
Básico	Otros datos de carácter personal

El cumplimiento de la LOPD y el acceso a la información contenida en el Documento Electrónico son elementos independientes entre sí, por lo que, en caso de duda, se impondrá siempre el más restrictivo.

2.5.5.2.2. Mecanismos para el acceso parcial a información restringida

Con el fin de favorecer el acceso a la información contenida en la entidad documento de acceso restringido, en los casos en que exista la posibilidad y modalidad de disociación de datos o acceso parcial, se deben incluir aquellas medidas propuestas para favorecer el acceso a la información de acceso restringido. Como referencia, se puede utilizar la siguiente tabla:

Denominación	**Definición**
Enmascaramiento de datos	Copia del documento en la que se han ocultado los datos susceptibles de protección.
Despersonalización o disociación	Copia del documento en la que se han ocultado los datos que identifican o permiten identificar fácilmente a las personas afectadas.
Exclusión de documentos para acceso parcial	Retirada de consulta pública de documentos concretos cuando se pueda ofrecer un acceso parcial al expediente, sin que resulte una información distorsionada o carente de sentido.
Limpieza de metadatos	Borrado o modificación de los datos de autor, localización,

	aplicación o sistema de origen, etc.

En estos casos, a la hora de la consulta, se proporcionará el documento al destinatario con carácter de copia electrónica parcial auténtica, tal y como se define en el anexo X, Copiado auténtico de documentos.

2.5.5.3. Requisitos de seguridad en el acceso a la información contenida en el SGDE/SGDEA

Se aplicarán aquellos mecanismos propios de los SGDE/SGDEA para evitar el acceso no autorizado a la información, así como, todas las directrices establecidas por el ENS, regulado por el Real Decreto 3/2010, en sus artículos 16, Autorización y control de accesos, art. 21 Protección de la información almacenada y en tránsito, y art. 23, Registro de actividad, que se concretan en las medidas op.acc, Control de acceso, y mp.info, Protección de la información.

El Acceso seguro al SGDE/SGDEA comprenderá dos operaciones sucesivas: la autenticación y la autorización.

La autenticación consiste en que el usuario que pretende acceder al sistema proporcione unas credenciales para que sea posible verificar su identidad. Hay dos formas principales de completar la autenticación en un SGDE/SGDEA:

- Proporcionando un par usuario/contraseña que habrá sido previamente registrado por el administrador del SGDE/SGDEA. Cuando se utilice esta alternativa, el SGDE/SGDEA debería implementar unas normas de seguridad básicas: almacenar las contraseñas previamente cifradas, establecer reglas de complejidad de las contraseñas y su caducidad periódica, limitar el número de intentos fallidos de entrada al sistema, registrar estos intentos y no proporcionar información detallada del motivo por el que se rechazan los mismos.
- Delegando la autenticación en el sistema operativo o red corporativa en la que está ejecutándose el SGDE/SGDEA. En este caso, el usuario se habrá autenticado previamente en dicho sistema o red, donde con su credencial se determina que tiene acceso al SGDE/SGDEA y se le franquea dicho acceso sin necesidad de volver a identificarse (mecanismos conocidos técnicamente como "Single Sign-On"). Éste es el medio recomendado por simplificar considerablemente la gestión de identidades en la organización.

La autorización se aplica una vez realizada con éxito la autenticación. A partir de la identidad verificada del usuario, se comprueba a qué recursos del SGDE/SGDEA está autorizado a acceder y qué operaciones puede efectuar en cada recurso concreto. La autorización será proporcionada por el SGDE/SGDEA e irá acompañada de un registro de todas las operaciones que modifiquen algún recurso o consulten recursos especialmente protegidos, lo que servirá como evidencia en las labores de auditoría de seguridad del SGDE/SGDEA y su contenido.

El SGDE/SGDEA debe proporcionar medidas técnicas para asegurar las siguientes dimensiones de la seguridad:

- Confidencialidad: mediante el mecanismo de autorización proporcionará acceso a cada recurso exclusivamente a las personas expresamente autorizadas, mediante su pertenencia a "listas blancas". Además, los recursos especialmente protegidos se guardarán cifrados.

- Integridad: La firma electrónica de documentos permite asegurar su integridad. Adicionalmente, la integridad, se puede asegurar mediante el cálculo sobre el contenido del elemento y almacenamiento de una función resumen (*hash*)
- Disponibilidad: esta dimensión suele garantizarla la infraestructura de red en la que se aloja el SGDE/SGDEA. Adicionalmente, se pueden recomendar instalaciones balanceadas o en *cluster* del SGDE/SGDEA que proporcionen alta disponibilidad y permitan distribuir picos de trabajo.
- Trazabilidad: de forma complementaria a la información proporcionada por los metadatos, el SGDE/SGDEA mantendrán registros de auditoría (*logs*) de aquellas acciones de los usuarios que se consideren más relevantes para la investigación de posibles incidentes de seguridad, como se mencionó más arriba, o cuyo registro sea obligatorio en virtud de una norma.

Otras medidas de seguridad adicionales, como la política de copias de seguridad, estarán delegadas en las infraestructuras comunes de la organización.

En función de los niveles de acceso a la información contenida en cada documento, se adoptarán las medidas de protección indicadas en su correspondiente categoría, así como en las inferiores, recogidas en la tabla del anexo III, Niveles de acceso del documento electrónico y medidas de protección.

Además, habrá que tener en cuenta que aquellos documentos que puedan salir del ámbito de la organización y contengan datos especialmente sensibles, pueden conllevar la adopción de medidas que eviten la indexación en los buscadores de Internet. Se recomienda someter cada uno de estos documentos a un proceso de limpieza de metadatos de archivo, que aseguren el borrado de la información relacionada con el autor, la aplicación, el sistema operativo en que se ha creado, etc.

2.5.5.3.1. Acceso a los expedientes y documentos electrónicos

La consulta del contenido del documento se realizará una vez cotejado el permiso efectivo del usuario en relación al mismo. Se registrará, si es posible, el acceso de cada uno de los usuarios a los documentos de aquellas categorías que impliquen un acceso limitado, pero no necesariamente cada una de las operaciones de consulta que realice. Se recomienda, además, el registro de las denegaciones de lectura, de cara a permitir realizar labores de auditoría de intentos de acceso no permitidos.

2.5.5.3.2. Establecimiento y modificación del nivel de acceso a la información

El nivel de acceso a la información se establece en el momento de incorporación de un documento al SGDE de la Organización.

Cada categoría documental, serie documental, del Cuadro de Clasificación o Repertorio de Series Documentales de la Organización tendrá establecido un nivel de acceso mínimo, nivel “por defecto”, que se asignará automáticamente al documento en el momento de su incorporación al SGDE.

A aquellos documentos que, en el momento de ser incorporados, no se les pudiera asignar una categoría, se considerarán de libre acceso.

Para definir un primer nivel de acceso de los usuarios a la documentación, se deberá tener bien diferenciadas las diferentes etapas de la gestión documental. Los niveles de acceso se definirán tomando en consideración esta diferenciación. Se deberán tener en cuenta las tres etapas de la gestión documental.

- Etapa de tramitación. Se inicia con la apertura del expediente y finaliza con su cierre. Incluye la gestión de los documentos electrónicos mientras se está efectuando la tramitación de un asunto.
- Etapa de vigencia. Comprende desde el momento de cierre del expediente hasta el momento en que dejan de mantenerse efectivos sus valores legales, fiscales o jurídicos.
- Etapa de conservación permanente. Una vez hecha la disposición, aquella documentación que posee un valor informativo y/o histórico se deberá de conservar de manera permanente.

2.5.6. Calificación

Confluyen aquí dos acepciones de ”calificación”, una desde la perspectiva archivística y otra desde la perspectiva de seguridad (ENS). Siempre que se trate de la “calificación de la información” desde la perspectiva de la seguridad se incluirá la referencia a la medida [mp.info.2].

2.5.6.1. Documentos esenciales

Se entiende por documentos esenciales aquellos que resultan indispensables y vitales para que una organización pueda alcanzar sus objetivos, cumplir con sus obligaciones diarias de servicio y respetar la legalidad vigente y los derechos de las personas.

La categorización del sistema (ENS, Anexo I), el ”Análisis de riesgos [op.pl.1]”, y la ”Calificación de la información [mp.info.2]“ aportarán criterios para identificar documentos esenciales y las medidas de seguridad y nivel requerido aplicables.

Cada departamento, organismo o entidad de la Generalitat decidirá cuáles son los documentos que cumplen estos requisitos y deben considerarse esenciales. Una vez identificados, se deberán adoptar las medidas necesarias para asegurar especialmente su confidencialidad, integridad, disponibilidad y autenticidad.

A nivel orientativo, se considera que los documentos electrónicos que podrían ser calificados como esenciales son aquellos que:

- Informan de las directrices, estrategias y planificación de la organización.
- Recogen derechos de la organización, singularmente relativos a convenios y documentos de propiedad.
- Recogen información sobre los edificios, instalaciones y sistemas de la organización.
- Dejan constancia de los acuerdos y resoluciones de los órganos de gobierno de la organización, tanto colegiados como unipersonales.
- Contienen datos necesarios para la protección de los derechos civiles, profesionales, financieros, jurídicos u otros derechos de los individuos u otras instituciones de la propia organización.
- Contienen elementos de prueba de las actividades presentes y pasadas de la organización para cumplir las obligaciones de rendición de cuentas.

La conselleria competente en materia de Tecnologías de la Información y la Comunicación, tomando como referencia el ENS, ha dimensionado los documentos esenciales según su nivel de:

Confidencialidad: Se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

- **Nivel bajo**. Porque su revelación causaría algún perjuicio o porque su revelación causaría pérdidas económicas apreciables.
- **Nivel Medio**. Porque su revelación causaría un daño importante aunque subsanable o porque su revelación causaría pérdidas económicas importantes.
- **Nivel Alto**. Porque su revelación causaría grave daño, de difícil o imposible reparación o porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas.

Integridad: Se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

- **Nivel bajo**. Porque su modificación no autorizada causaría algún perjuicio o porque su modificación no autorizada causaría pérdidas económicas apreciables.
- **Nivel Medio**. Porque su modificación no autorizada causaría un daño importante aunque subsanable o porque su modificación no autorizada causaría pérdidas económicas importantes.
- **Nivel Alto**. Porque su modificación causaría grave daño, de difícil o imposible reparación o porque su modificación causaría pérdidas económicas elevadas o alteraciones financieras significativas.

Autenticidad: Se establecerá en función de las consecuencias que tendría el hecho de que su origen o el destinatario de la información fuera falso.

- **Nivel bajo**. Porque la falsedad en el origen o en su destinatario causaría algún perjuicio o porque la falsedad en su origen o en su destinatario causaría pérdidas económicas apreciables.
- **Nivel Medio**. Porque la falsedad en el origen o en su destinatario causaría un daño importante aunque subsanable o la falsedad en el origen o en su destinatario causaría pérdidas económicas importantes.
- **Nivel Alto**. Porque la falsedad en el origen o en su destinatario causaría grave daño, de difícil o imposible reparación o porque su la falsedad en el origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas.

Disponibilidad: Se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.

- **Nivel bajo**. Tiempo máximo con el servicio interrumpido: entre 1 y 5 días.
- **Nivel Medio**. Tiempo máximo con el servicio interrumpido: entre 4 horas y 1 día.
- **Nivel Alto**. Tiempo máximo con el servicio interrumpido: menor de 4 horas.

La gestión de los documentos calificados como esenciales requerirá:

- Obtención de una copia electrónica auténtica según lo dispuesto en el anexo X, sobre copiado auténtico de documentos
- El tratamiento y conservación, en su caso, de original y copia, teniendo en cuenta que básicamente pueden darse tres circunstancias en relación con los soportes:
  - El documento original es electrónico.
  - El original es en soporte papel.
  - El expediente es híbrido, es decir en soporte papel y electrónico.

El tratamiento y conservación, en su caso de original y copia, será según lo establecido en el procedimiento o estrategia de conservación de la Generalitat.

En todos los casos, se adoptarán las medidas necesarias para que exista una réplica del documento electrónico o una copia auténtica y garantizar las condiciones de protección requeridas.

Cuando se trate de un documento esencial cuyo original está en soporte papel, una vez realizada la copia electrónica auténtica, el original en papel será objeto de estudio de valoración junto con su serie documental.

Si se trata de documento esencial que forma parte de un expediente que se conserva íntegramente en papel, se realiza una copia electrónica auténtica. El original en papel continuará conservándose en dicho formato en el expediente, mientras no haya un dictamen de la JCDA de sustitución de soporte para toda la serie documental.

Si se trata de un documento esencial que forma parte de un expediente híbrido, se realizará una copia electrónica auténtica del mismo y se adoptarán las medidas necesarias para garantizar las condiciones de protección necesarias.

En los departamentos de la Administración de la Generalitat y otros entes incluidos en el ámbito de aplicación de esta Política, los documentos esenciales se reflejan en el elemento 13.4 del e-EMGDE. Los documentos esenciales deben estar previamente identificados. En ese caso, los metadatos se asignarán en el momento de su captura o incorporación al SGDE. No obstante, este metadato se podrá incorporar en cualquier momento del proceso si la organización no contase con una identificación previa de los documentos esenciales o se produjesen cambios en la normativa que dispusieran que un documento previamente no identificado como tal pasase a convertirse en documento esencial.

2.5.6.2. Valoración

La valoración documental es un proceso para determinar los valores de los documentos producidos y/o conservados por los departamentos de la Administración de la Generalitat y otros entes incluidos en el ámbito de aplicación de la PGDE-GV, a través del análisis contextual de los mismos, y que dará como resultado el establecimiento de plazos de conservación, transferencia y acceso de las series documentales estudiadas.

En la Generalitat, la valoración documental corresponde a la Junta Calificadora de Documentos Administrativos (JCDA), que es el órgano colegiado autorizado para dictaminar sobre la valoración, conservación y/o eliminación de la documentación que conservan los archivos de la Comunitat Valenciana.

La JCDA dispone de un portal propio donde se puede encontrar toda la información sobre sus funciones, procedimiento, documentación, etc. La url es la siguiente: http://www.jqda.cult.gva.es

La valoración documental consiste en el estudio y análisis de las características históricas, administrativas, jurídicas, fiscales e informativas de las series documentales, las **comisiones de valoración documental,** creadas en las instituciones valencianas (*conselleries*, ayuntamientos, universidades...) son las **encargadas de realizar las propuestas de valoración** para presentarlas a la JCDA.

En la determinación del valor de los documentos de archivo con vistas a su conservación en soporte original o alternativo o a su posible eliminación se tendrán en cuenta los criterios de la JCDA.

Determinando los valores de la serie documental se fijan los criterios relativos a los tres ámbitos siguientes:

- Los plazos de transferencia entre los distintos archivos responsables del sistema. Las transferencias de documentos tienen el carácter de un procedimiento administrativo especial de las Administraciones Públicas consistentes en la entrega, ordenada y relacionada por escrito, de los documentos de un archivo a otro, así como del traspaso de las responsabilidades relativas a su custodia y conservación.
- Los plazos de conservación o eliminación total o parcial de la serie, así como el cambio de soporte.
- Los plazos de acceso, que se incluyen en la valoración de la JCDA . La información se completa con el informe sobre el acceso a la documentación que se adjunta a la presentación de la propuesta.

El calendario de conservación es el listado de propuestas de valoración que han sido aprobadas por la JCDA. Se trata de un listado donde se incluye el número de registro, el código de tabla, denominación de la serie, estado y productor. Proporciona datos sobre términos de transferencias al Archivo Central, Archivo Intermedio e Histórico.

Las propuestas del dictamen de conservación y eliminación corresponden a la Comisión de Valoración Documental y deben ser elevadas a la JCDA para su dictamen preceptivo y vinculante.

Según la norma ISO 23081-2:2011, los propios metadatos para la gestión de documentos deben ser objeto de valoración. La valoración determina no sólo qué metadatos deben capturarse acerca del documento, sino durante cuánto tiempo deben conservarse.

En lo que respecta a los metadatos, a medida que se vaya disponiendo de la información, se cumplimentarán los elementos:

- 13.1. Valoración.
  - 13.1.1. Valor primario.
    - 13.1.1.1. Tipo de valor (administrativo, legal, fiscal)
    - 13.1.1.2. Plazo (Legislación en la que se basa)
  - 13.1.2. Valor secundario del e-EMGDE (informativo, histórico).

Por ejemplo, el valor primario y el plazo (valor fiscal, cuatro años) es una información que se puede proporcionar desde el momento de creación o incorporación de la entidad documento al sistema de gestión

documental, pero hay otra información que no siempre es posible incorporar hasta la elaboración y aprobación de los correspondientes calendarios de conservación o, en su caso, la existencia de un dictamen por parte de la autoridad calificadora.

La valoración documental tendrá también en cuenta la política de seguridad de la información de la Generalitat, en la que se valora el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas.

Los pasos para la selección de medidas de seguridad se estructuran en 6 puntos.

1. Identificación de los tipos de activos presentes.
2. Identificación de información manejada, su tipo y nivel.
3. Determinación de las dimensiones de seguridad relevantes.
4. Determinación del nivel correspondiente a cada dimensión de seguridad.
5. Determinación de la categoría del sistema.
6. Selección de las medidas de seguridad apropiadas.

La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad firmado por el responsable de la seguridad del sistema y que habrá que coordinar con la JCDA.

2.5.6.3. Dictamen

La JCDA emite, como autoridad calificadora y en función de los plazos de conservación propuestos o resultantes del proceso de valoración documental, un dictamen favorable o desfavorable referido a la transferencia (apartado 2.5.8), conservación (apartado 2.5.7.), eliminación (apartado 2.5.9) o acceso (apartado 2.5.5) de las series documentales que queda recogido en el listado de propuestas de valoración documental de la Generalitat.

La JCDA examinará los expedientes de las propuestas de las tablas de valoración documental por orden de recepción, aplicando los criterios generales que haya elaborado la propia Junta, y emitirá el dictamen correspondiente.

Estudiados los valores de cada serie documental, siguiendo los criterios utilizados en la fase de valoración, se pueden establecer las propuestas de dictamen siguientes:

- Conservación permanente.
- Eliminación parcial, cuando se conservan parte de los expedientes o una muestra de los mismos de acuerdo con diferentes métodos de muestreo. En este caso se ha de hacer constar el tipo de eliminación parcial.
- Eliminación total, en el caso de series documentales sin valor secundario, histórico o informativo y cuya información está recogida en otras series documentales o no es necesaria su conservación.

Se entiende por muestreo la técnica de selección según criterios sistemáticos (numéricos, alfabéticos, topográficos) o cualitativos, de una cierta proporción de documentos en representación de un conjunto, utilizando como métodos:

Ejemplar o testigo	Selecciona un expediente dentro de una serie documental para ilustrar la práctica administrativa del momento.
Cualitativo o selectivo	Método subjetivo que se basa en criterios preconcebidos de antemano, mediante los cuales se conservan los documentos que se consideran más importantes.
Sistemático	Se establece un criterio previo de selección (numérico, cronológico, geográfico o alfabético) de expedientes, dependiendo de la organización de la serie documental.
Aleatorio	Criterio por el que se seleccionan varios expedientes al azar, teniendo en cuenta que cualquiera de ellos tiene las mismas cualidades para representar al conjunto de la serie documental.

Una vez aprobada la propuesta de dictamen por parte de la JCDA, se publican mediante resolución de la conselleria competente en materia de archivo, que incluye los siguientes datos:

- Código
- Serie documental
- Órgano productor
- Función
- Fecha dictamen

En cuanto al dictamen:

- 13.2. Dictamen.
  - 13.2.1. Tipo de dictamen.
  - 13.2.2. Acción dictaminada.
  - 13.2.3. Plazo de ejecución de la acción dictaminada del e-EMGDE, una vez aprobada la propuesta de dictamen.

2.5.7. Conservación

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 JCDA y a lo dispuesto en la estrategia de conservación implantada en la Generalitat.

Atendiendo a lo dispuesto en el ENS y, proporcionalmente a los riesgos a los que estén expuestos los documentos, la Generalitat contará con un plan de continuidad para preservar los documentos y expedientes electrónicos conservados, así como sus metadatos asociados, que incluirá lo previsto en el anexo II del ENS sobre copias de seguridad (backup) [mp.info.9]; junto con las medidas de protección de la información [mp.infor], de protección de los soportes de información [mp.si] del citado anexo II, y, en cualquier caso, las medidas de protección de datos de carácter personal según lo dispuesto en la LOPD y su normativa de desarrollo, el Decreto 220/2014 por el que se aprueba el Reglamento de Administración

Electrónica de la Comunitat Valenciana, la Ley 4/1998 del Patrimonio Cultural Valenciano, y la regulación de la JCDA y el procedimiento de valoración, conservación y eliminación del patrimonio documental de los archivos públicos.

Para prevenir riesgos de pérdida física de los documentos o de su valor probatorio, la Generalitat debe definir un Plan de Preservación de los Documentos Electrónicos de la organización que incorporará un análisis y gestión de riesgos en el ámbito de la gestión documental. Desde la Generalitat se ha llevado a cabo el estudio del ciclo de cumplimiento del ENS en el que se llevan a cabo las siguientes acciones:

- Preparar y aprobar la política de seguridad. Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat.
- Valorar/categorizar el sistema: información/servicios.
- Realizar análisis de riesgos (MAGERIT).
- Preparar y aprobar la declaración de aplicabilidad.
- Definir roles y asignar personas. Decreto 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat.
- Implantar, operar y monitorizar el sistema.
- Auditar cada dos años.
- Mejorar la seguridad.

Los roles definidos en nuestra Política de Seguridad se dividen en tres niveles:

- **Gobierno**. Determinan los requisitos de seguridad de la información y los servicios y datos personales. En cuanto al ENS, lo integran el Responsable de la información, el Comité de Seguridad de la Información y el Responsable del Servicio, y para la LOPD, el Responsable de ficheros LOPD.
- **Ejecutivo**. Determinan las decisiones para satisfacer los requisitos de seguridad de la información, servicios y datos personales. Está formado por el Responsable de seguridad, en cuanto al ENS y por el Responsable de Seguridad LOPD, para la LOPD.
- **Operaciones**. Planificar e implantar las medidas de seguridad, así como monitorizar y gestionar la seguridad. En cuanto al ENS, lo integran el Responsable del Sistema y los Administradores del Sistema, y para la LOPD, los Administradores de la Seguridad LOPD.

La Ley de Patrimonio Cultural y la Ley de Archivos obligan a la conservación del patrimonio documental. Para el cumplimiento del ENS, la Generalitat, ha dividido su proceso de adecuación en cuatro fases, de las cuales la primera de ellas corresponde a esta actuación. Estas **cuatro fases** son las siguientes:

- En la **primera fase** se llevaran a cabo la identificación y la valoración de los servicios.

  En esta fase, se debe identificar tanto la información como los servicios que se prestan. Una vez identificados deben ser valorados por sus respectivos responsables. En base a esta valoración el Responsable de Seguridad decidirá qué medidas y controles se deben implantar.

Además, se debe realizar el análisis e identificación de riesgos sobre los activos mediante la elaboración de un Informe o Tabla de Evaluación de Riesgos, que incluya los riesgos identificados, y por cada uno de ellos, sus consecuencias e impacto, su escala de gravedad y de probabilidad o frecuencia y el tratamiento de los mismos.

A nivel de archivos también se llevan a cabo dichas tareas, valorando la documentación generada en el desempeño de sus funciones, por los distintos servicios y emitiendo un dictamen de dicha valoración.

- En la **segunda fase** se realizará un análisis de riesgos y una declaración de aplicabilidad, que estará basada en la metodología Magerit V3, la cual servirá de indicador para analizar el nivel de cumplimiento del ENS.
- La **tercera fase** estará dedicada al plan de mejora de la seguridad.
- Y la **cuarta fase** corresponde al plan de mantenimiento y mejora del sistema.

Las medidas de prevención que se adopten para cada tipo o grupo de riesgos se obtendrán mediante la categorización del sistema de información, en el que hay que conseguir un equilibrio entre la importancia del mismo y el esfuerzo dedicado a la seguridad.

Según el ENS, la determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas. Se definen **tres categorías**:

- **Básica.** Un sistema de información en el que alguna de sus dimensiones de seguridad alcanza el nivel Básico y ninguna alcanza un nivel superior.
- **Media**. Un sistema de información en el que alguna de sus dimensiones de seguridad alcanza el nivel Medio y ninguna alcanza un nivel superior.
- **Alta**. Un sistema de información en el que alguna de sus dimensiones de seguridad alcanza el nivel Alto.

En este sentido, la valoración documental, será determinante en dicha categorización. La JCDA, fijará los plazos de conservación de los documentos y las series documentales, que podrán ser definitivos o temporales.

Este Plan de Preservación garantizará la accesibilidad, autenticidad, disponibilidad, integridad, trazabilidad, inteligibilidad y legibilidad de los documentos electrónicos a lo largo de su ciclo de vida, frente a los siguientes grupos de riesgos:

- Los derivados de la continua evolución de la tecnología y la consiguiente obsolescencia de la misma.
- Los que son consecuencia de un mal funcionamiento o de un uso erróneo de la tecnología, y que pueden ocasionar la pérdida o degradación de los documentos electrónicos, total o parcialmente.
- Los que proceden de una posible descontextualización de los documentos electrónicos.

- Los que forman parte del ámbito de la seguridad de las TIC y que pueden suponer una alteración intencionada de los documentos electrónicos o su misma desaparición (accesos no permitidos, ataques, robo de soportes, etc.).
- Los que directa o indirectamente derivan del aumento constante del volumen de documentos y en paralelo de los costes necesarios para asegurar el entorno adecuado de conservación.

La Ley 3/2005 de Archivos, establece que toda la documentación electrónica generada o recibida por cualquier organismo de la Administración Pública forma parte del Patrimonio Documental, sin perjuicio del momento de su generación, y que su eliminación deberá ser autorizada por la autoridad calificadora competente, la JCDA. En ningún caso se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos. El proceso de eliminación debe seguir la metodología fijada por dicha Junta.

El Sistema de Gestión de Documentos Electrónicos asegurará la accesibilidad, disponibilidad, integridad y autenticidad de los documentos electrónicos que se encuentran en él, independientemente de los soportes de almacenamiento o los formatos de los ficheros.

2.5.7.1. Trazabilidad de los documentos electrónicos.

El SGDE utilizado en la organización deberá asegurar la trazabilidad de las acciones que se realicen sobre los documentos almacenados en el sistema. Como mínimo, los eventos que se registrarán sobre cada documento almacenado en el SGDE serán los siguientes:

- La creación del documento.
- La modificación y versionado del documento (creando nuevas versiones).
- El borrado físico del documento.
- La transferencia del documento a otro SGDE con cambio de custodia.
- El acceso al contenido del documento, cuando dicho documento tenga un nivel de control de acceso a la información con una categoría de seguridad con el nivel de confidencialidad más alto.

La trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido o modificado una cierta información:

- **Nivel básico:** porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores o porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de perseguir delitos.
- **Nivel Medio:** porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error importante o porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad de perseguir delitos.
- **Nivel Alto:** porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave o porque la incapacidad para rastrear un acceso a la información dificultaría muy notablemente la capacidad de perseguir delitos.

En el caso de los expedientes electrónicos, los eventos que se registrarán en el SGDE referidos a la trazabilidad son:

- La creación del expediente electrónico y su índice.
- La incorporación de nuevos elementos -documentos u otros expedientes- al expediente y modificación del índice electrónico.
- La retirada de elementos -documentos u otros expedientes- del expediente y la consiguiente modificación de su índice electrónico.
- El cierre del expediente y del índice electrónico, sin posibilidad de agregar o eliminar más elementos.
- La transferencia del expediente a otro SGDE con cambio de custodia.
- La eliminación física del expediente.

En un entorno multientidad, tal y como se propone en esta Política, se establecerán las adecuadas relaciones con las entidades Actividad, Regulación y Agente pertinentes. En este sentido, se contemplarán diferentes aspectos relativos a la trazabilidad, tales como:

- Indicador de tipo de acción (e-EMGDE21.1 – Acción): debe establecerse una relación con la entidad Actividad.
- Razón por la que se lleva a cabo la acción asociada (e-EMGDE21.2 – Motivo reglado): debe establecerse una relación con la entidad Regulación.
- Identificación del usuario que ha realizado la Acción (e-EMGDE21.3 – Usuario de la acción): debe establecerse una relación con la entidad Agente.
- Explicación de la Acción (e-EMGDE21.4 – Descripción): debe cumplimentarse en todas las entidades.
- Información que registra la autoría y la fecha de los posibles cambios que han sufrido los metadatos de una entidad, una vez realizada la acción (e-EMGDE21.5 – Modificación de los metadatos): debe cumplimentarse en todas las entidades.
- Información que registra el elemento de metadato que ha sido modificado sobre una determinada entidad y su valor anterior (e-EMGDE21.6 – Historia del cambio): debe cumplimentarse a la entidad Relación.

Al completarse cada uno de los eventos anteriores, el SGDE generará los metadatos que se indican abajo como necesarios para una óptima gestión documental, con el formato especificado en el e-EMGDE-GV, y los registrará como metadatos asociados al propio documento o al índice electrónico asociado al expediente. Estos metadatos podrán custodiarse en un repositorio diferente al del SGDE, manteniendo en todo momento su relación con el documento o expediente electrónico al que se refieren.

En el caso de las series documentales incluidas en los procesos archivísticos de transferencia, los metadatos obligatorios se acompañarán de los metadatos complementarios necesarios e imprescindibles, para una correcta gestión documental, que se desglosan en el anexo II, del perfil de metadatos institucional y que se refieren también al apartado 2.5.8. Transferencia.

Cuando se complete la eliminación física de un documento/expediente, deberá mantenerse una referencia al mismo en el SGDE o en otro repositorio externo a la que estén asociados todos los eventos registrados durante la vida útil del documento. Esta referencia se mantendrá de manera permanente en la categoría en la entidad Documento, categoría Serie, pudiéndose eliminar en la categoría Expediente/Documento en los plazos marcados por la resolución pertinente de la JCDA.

Los metadatos para la información de auditoría que se registrarán de estos eventos son los siguientes:

Metadatos	Elemento e-EMGDE	Contenido	Obligatorios/ Necesarios
Acción	e-EMGDE21.1	Tipo de actuación realizada sobre el documento	Sí
Fecha de la acción	e-EMGDE21.1.1	Fecha y hora en que se produce la actuación	Sí
Entidad de la acción	e-EMGDE21.1.2	Elemento del documento (parte del documento, metadato…) al que se limite la actuación. Cuando no se informe este metadato, se entiende que la actuación afecta al documento completo.	Sí
Motivo Reglado	e-EMGDE21.2	Razón o disposición legal/reglamentaria o procedimiento por el que se lleva a cabo la actuación	Sí
Usuario de la acción	e-EMGDE21.3	Identidad del usuario que realiza la actuación, utilizando cualquier atributo que lo identifique de forma inequívoca (nombre de red, IP, DNI…)	Sí
Modificación de los metadatos	e-EMGDE21.5	Información que registra la autoría y la fecha de los posibles cambios	Sí
Historia del cambio	e-EMGDE21.6	Información que registra el elemento de metadato que ha sido modificado	Sí
Nombre del elemento	e-EMGDE21.6.1	Nombre de elemento o sub-elemento de metadato cuyo valor ha sido modificado	Sí
Valor anterior	e-EMGDE21.6.2	Contenido anterior de un elemento o sub-elemento de metadato que ha sido modificado.	Sí

En el caso del SGDEA, se registrarán los eventos de:

- Incorporación de un nuevo documento/expediente por cambio de custodia desde el SGDE.
- Eliminación física de un documento/expediente, con obligatoriedad en este caso de informar el metadato “Motivo reglado”.
- Consulta de un documento con el nivel más alto de confidencialidad, siempre que no hubiera expirado esa cualidad.
- Así como cualquier otra acción recogida en el Apéndice 7 (Esquema de nombres de relaciones de acciones de gestión de documentos – extensible) del e-EMGDE que permita una gestión óptima de los documentos.

2.5.8. Transferencia

La transferencia es el "procedimiento habitual de ingreso de fondos en un archivo mediante traslado de las fracciones de series documentales, una vez que éstas han cumplido el plazo de permanencia fijado por las normas establecidas en la valoración para cada una de las etapas del ciclo vital de los documentos". Tiene como objetivo facilitar el paso de los documentos a través de las fases de archivo del sistema, de manera que puedan recibir el tratamiento adecuado en cada momento de su ciclo de vida.

En este sentido, se contemplan dos escenarios posibles:

- Transferencia de custodia con cambio de repositorio.
- Traspaso de responsabilidad de la custodia y gestión sin cambio en el repositorio.

De toda transferencia deberá quedar constancia de los movimientos efectuados mediante metadatos de trazabilidad.

De conformidad con lo previsto en el Apartado V.6. de la NTI de Expediente Electrónico y en el Apartado VII.5. de la NTI de Documento Electrónico, en caso de intercambio de expedientes electrónicos entre Administraciones Públicas que suponga una transferencia de custodia o traspaso de la responsabilidad de la gestión de expedientes y documentos que deban conservarse permanentemente, el órgano o entidad transferidora será la responsable de verificar la autenticidad e integridad del expediente en el momento de dicho intercambio, mediante la firma electrónica de los índices de los expedientes y de los documentos electrónicos.

Por otra parte, la NTI de Política de Gestión de Documentos Electrónicos en el apartado VI relativo a Procesos de Gestión de Documentos electrónicos, en su punto 8 establece "la transferencia de documentos incluirá las consideraciones para la transferencia entre repositorios, así como las responsabilidades en cuanto a su custodia".

Asimismo, cuando la transmisión se realice mediante soportes físicos, deberán tenerse presentes en el proceso de transferencia las medidas de Protección de los soportes de información [mp.si] previstas en el ENS (en particular las referidas a su transporte y a los mecanismos que relacionados con la integridad y la trazabilidad) y en el resto de la normativa que pueda ser de aplicación.

La transferencia entre repositorios debe estar definida y controlada por reglas en el SGDE, a partir de lo dispuesto en los calendarios de conservación. Además, debe disponerse de mecanismos de bloqueo para aquellos expedientes o documentos que deban exceptuarse de la aplicación de las reglas generales por algún motivo, por ejemplo, porque forman parte de un recurso abierto.

Los metadatos del documento electrónico deben ser transferidos asociados al documento para permitir su identificación, su autenticidad y los procedimientos de conservación

Además de los metadatos y firmas correspondientes, los documentos deben ir acompañados de otra información complementaria:

- Indicaciones sobre procedimientos de privilegios de uso y acceso.
- Indicaciones sobre procedimientos para prevenir, corregir y descubrir pérdidas de información o alteración de los documentos.
- Indicaciones sobre procedimientos de conservación en relación al deterioro de los soportes y la obsolescencia tecnológica.

Al igual que en el caso de los archivos físicos, se recomienda la definición de un protocolo de transferencia de documentos y expedientes electrónicos a archivos centrales e intermedios, que comprenderá como mínimo:

- Añadir las firmas que pudieran faltar, así como la información necesaria para la verificación y validación y los sellos de tiempo que garanticen la conservación a largo plazo de las mismas, si fuera necesario, a no ser que la transferencia se produzca a un sistema que garantice la conservación de las firmas por otros medios.
- Revisar la documentación y actualizar y completar los metadatos mínimos necesarios para la transferencia de documentos y expedientes electrónicos con cambio de custodia.
- Adaptar los documentos que vayan a enviarse, preferiblemente, a un formato longevo recogido en la NTI de Catálogo de Estándares, incluyendo aquellas migraciones o cambios de formato que sean pertinentes.

En el caso de la transferencia física, deberá quedar constancia de la remisión de los expedientes y documentos por parte del órgano o aplicación emisora de los mismos y de su recepción en el archivo de destino. El receptor deberá verificar el contenido de la transferencia, confirmando que contiene los expedientes y documentos acordados, en el formato correcto y con los metadatos complementarios necesarios. Una vez hecha dicha comprobación, deberá enviar constancia de la recepción correcta al organismo que realizó la transferencia.

El SGDEA deberá poder realizar informes sobre los expedientes ingresados en el archivo receptor por series documentales, con mención del órgano remitente, la identificación de los expedientes, sus fechas extremas y la fecha de ingreso en el archivo. Con los informes elaborados podrá generarse un Registro General de entrada de fondos, como instrumento de control del archivo.

En el caso de que la transferencia física suponga una duplicación de los documentos que son objeto de la misma, el órgano remitente, una vez obtenida la conformidad del nuevo responsable de la custodia, deberá proceder al borrado de sus propios ejemplares.

En el caso de que se remita al archivo documentación en soporte papel como parte de expedientes híbridos, deberá ir acompañada de la oportuna Relación de entrega, que quedará consignada en el Registro General de entrada de documentos del archivo receptor, tras el cotejo de dicha documentación. La vinculación en los expedientes híbridos entre los documentos en soporte papel y electrónicos no se debe perder.

En caso de crearse un archivo electrónico único para la Administración de la Generalitat, según lo dispuesto en el artículo 18.2 de la Ley 3/2005 y en consonancia con el art. 20 del Real Decreto 1708/2011 referido a

la Administración General del Estado, debe transferirse la responsabilidad de la custodia y gestión de los documentos y expedientes electrónicos contenidos en el mismo a los archivos centrales de las *conselleries* o al archivo histórico, Archivo Histórico de la Comunitat Valenciana, para su adecuada conservación y tratamiento archivístico, así como para facilitar su consulta por parte de los ciudadanos y de la investigación histórica.

A tal efecto, se arbitrarán las soluciones técnicas adecuadas y se proporcionarán los permisos de acceso y gestión necesarios a los responsables del Archivo Histórico de la Comunitat Valenciana y, en su caso, de los archivos centrales e intermedios de las *conselleries*, con el fin de que se garantice para generaciones futuras la contextualización y conservación de los documentos electrónicos y sus metadatos asociados.

A continuación, se incluye un listado de los metadatos complementarios mínimos necesarios para la transferencia de documentos y expedientes electrónicos, que serán incorporados en el SGDE/SGDEA en la entidad documento en los hitos de los procesos en los que se produce transferencia física o transferencia de la responsabilidad de la custodia y gestión, es decir, en las transferencias de los archivos de oficina a los archivos centrales del departamento, de los archivos centrales al archivo histórico. También se incluyen en este listado los metadatos relativos a trazabilidad que tienen carácter de recomendados:

- e-EMGDE1 - Categoría
- e-EMGDE4.2 - Fecha fin
- e-EMGDE8 - Seguridad
  - e-EMGDE8.4 - Sensibilidad datos de carácter personal
  - e-EMGDE8.5 – Clasificación ENS
  - e-EMGDE8.6 - Nivel de confidencialidad de la información
- e-EMGDE9 - Derechos de acceso, uso y reutilización
  - e-EMGDE9.1 - Tipo de acceso
  - e-EMGDE9.2 - Código causa de limitación
  - e-EMGDE9.3 - Causa legal/normativa de limitación
  - e-EMGDE9.4 - Condiciones de reutilización
- e-EMGDE13 - Calificación
  - e-EMGDE13.1 - Valoración
    - e-EMGDE13.1.1 - Valor primario
      - e-EMGDE13.1.1.1 - Tipo de valor
      - e-EMGDE13.1.1.2 - Plazo
    - e-EMGDE13.1.2 -Valor secundario
  - e-EMGDE13.2 - Dictamen
    - e-EMGDE13.2.1 Tipo de dictamen
    - e-EMGDE13.2.2 Acción dictaminada

        - e-EMGDE13.2.3 – Plazo de ejecución de la acción dictaminada
    - e-EMGDE13.3 – Transferencia
        - e-EMGDE13.3.1 - Fase de archivo
        - e-EMGDE13.3.2 - Plazo de transferencia
    - e-EMGDE13.4 - Documento esencial
- e-EMGDE21 – TRAZABILIDAD (recomendados para la transferencia)
    - e-EMGDE21.1 Acción
        - e-EMGDE21.1.1 -Descripción de la acción
        - e-EMGDE21.1.2 - Fecha de la acción
        - e-EMGDE21.1.3 – Entidad de la acción
    - e-EMGDE21.2 - Motivo reglado
    - e-EMGDE21.3 - Usuario de la acción
    - e-EMGDE21.5 - Modificación de los metadatos
    - e-EMGDE21.6 - Historia del cambio
        - e-EMGDE 21.6.1 - Nombre del elemento
        - e-EMGDE21.6.2 - Valor anterior
- e-EMGDE22 - CLASIFICACIÓN
    - e-EMGDE 22.2 – Denominación de clase
    - e-EMGDE22.3 – Tipo de clasificación (SIA/Funcional)
- e-EMGDE26 - IDENTIFICADOR DEL DOCUMENTO ORIGEN

Los metadatos relativos al acceso a los documentos que se han visto en el punto 2.5.4 tienen especial relevancia en los procesos de transferencia.

2.5.9. Destrucción o Eliminación

Los escenarios en los que se podrá realizar la destrucción física de la información almacenada en documentos/expedientes electrónicos son los siguientes:

- Destrucción de información como última fase de un procedimiento reglado de eliminación y destrucción, realizado con las formalidades del Decreto 189/2005, de 2 de diciembre, del Consell de la Generalitat, por el que se regula el procedimiento de valoración, conservación y eliminación de los documentos de las Administraciones Públicas de la Comunidad Valenciana y las series de los mismos, cualquiera que sea el tipo de soporte, con la finalidad de garantizar la protección del patrimonio documental de las Administraciones Públicas valencianas. Este hecho figurará en los dictámenes correspondientes a la serie documental.
- Cambio de soporte o formato como consecuencia de obsolescencia del formato anterior o fin de la

vida útil del soporte previo. En este caso, se realizará la destrucción o borrado de la información en el soporte o formato inicial.

- Transferencia con cambio de custodia a otro organismo o archivo. En el caso de que la transferencia suponga una duplicación de los documentos que son objeto de la misma, el órgano remitente, una vez obtenida la conformidad del nuevo responsable de la custodia, deberá proceder al borrado de sus propios ejemplares.

En los dos últimos escenarios, y siempre que se realicen copias auténticas de los documentos electrónicos con/sin cambio de formato con las exigencias del ENI, el marco normativo de aplicación será dicho Real Decreto y las Normas Técnicas de Interoperabilidad que lo desarrollan.

2.5.9.1. Pasos previos a la destrucción de la información

La eliminación de documentos requerirá el dictamen preceptivo de la JCDA.

Los procesos de destrucción o eliminación segura de documentación electrónica y soportes informáticos deben integrarse en la Política de Gestión de Documentos Electrónicos y la política de seguridad de la Generalitat y se atendrán al procedimiento establecido en el Decreto 189/2005.

A instancias de lo dictaminado por la JCDA, se iniciará el proceso de eliminación, respetando el procedimiento dictado por el artículo 18 del Decreto 189/2005, para lo cual se generará el expediente de eliminación correspondiente.

El expediente de eliminación, en el caso de la documentación relativa a la Generalitat, se comunicará a la JCDA, la cual lo revisará en la primera reunión que celebre y formulará las observaciones que estime pertinentes, comunicándolo posteriormente a los responsables de la custodia de la documentación en el plazo de diez días para que se proceda, si no hay ningún inconveniente, a su eliminación.

El órgano responsable de los documentos redactará el acta de eliminación, en la que acreditará que se han cumplido todos los requisitos previstos en el artículo 17 del Decreto 189/2005. En el acta deberá constar el lugar, fecha y duración de los trabajos de eliminación, procedimiento utilizado, personas intervinientes y funcionario fedatario de la operación.

El acta deberá firmarla el responsable del órgano que custodia la documentación y el archivero correspondiente.

Si la resolución dispone la conservación de los documentos o series documentales en soporte distinto al original, antes de proceder a la eliminación de dicho original deberán obtenerse copias auténticas en soporte diferente. En este caso, habrá de levantarse un acta complementaria a la prevista en el apartado 4 de este mismo artículo, y adjuntarse al expediente de eliminación.

Un duplicado del acta de eliminación se remitirá a la JCDA en el plazo de diez días siguientes a la fecha de las actuaciones correspondientes.

La JCDA llevará un Registro de todas las actas de eliminación documental.

La destrucción sólo se podrá llevar a cabo cuando se haya aprobado así en la tabla de valoración documental correspondiente por Resolución del órgano competente.

En ningún caso se podrá autorizar la eliminación ni se podrá proceder a la destrucción de documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas físicas o jurídicas o no hayan transcurrido los plazos que la legislación vigente establezca para su conservación.

En los expedientes y documentos afectados por estos procedimientos se incluirán los siguientes metadatos:

- e-EMGDE 21 - Trazabilidad.
  - e-EMGDE 21.1 Acción (Destruye o Elimina)
    - e-EMGDE 21.1.1 Descripción de la acción
    - e-EMGDE 21.1.2 Fecha de la acción.
    - e-EMGDE 21.1.3 Entidad de la acción.
  - e-EMGDE 21.2 Motivo reglado.
  - e-EMGDE 21.3 Usuario de la acción.

2.5.9.2. Aspectos técnicos relacionados con la destrucción de la información

Lo expuesto hasta ahora implica la necesidad de incluir en la gestión del documento un procedimiento de borrado seguro de los documentos electrónicos, en el que se distinguen dos posibles acciones:

- La eliminación de los ficheros que contienen los datos del soporte en que se almacenan, liberando así el espacio que ocupaban para su reutilización, pero de forma que se impida la reconstrucción posterior de la información eliminada. A esta acción la llamaremos "borrado seguro". Esta tarea se ejecutará en los siguientes casos:
  - Por aprobación de la eliminación del documento o expediente que lo contiene.
  - Por cambio de formato en el documento.
  - Por transferencia entre sistemas de gestión documental.
- La destrucción física del soporte, que impida la recuperación futura del contenido del mismo y su reutilización. A esta acción la llamaremos "destrucción segura". Esta situación se produce cuando se sustituye el soporte de almacenamiento, por obsolescencia o migración, y no sea posible completar el borrado seguro de la información contenida en el mismo. También se produce en el caso de soportes que no admiten la reutilización del espacio borrado (como los discos ópticos).

Considerando la metodología habitual de trabajo en la Administración, los procedimientos de borrado o destrucción deben incluir:

- Los dispositivos de almacenamiento local: disco duro del puesto de usuario, dispositivos móviles, dispositivos removibles como discos duros externos, memorias USB, tarjetas de memoria, etc.
- Los soportes de almacenamiento en red: accesibles mediante protocolos para compartir ficheros (CIFS o NFS), redes SAN, almacenamiento en la nube, etc.

De acuerdo con la clasificación establecida por el Centro Criptológico Nacional (CCN), distinguiremos los

niveles siguientes de borrado /destrucción de la información:

- Nivel 0: Borrado usando comandos/utilidades estándar del sistema operativo. Estas técnicas generalmente marcan el espacio ocupado por los archivos a borrar como disponible, pero no eliminan realmente el contenido almacenado. Por este motivo, no impide la recuperación posterior de la información borrada ni proporcionan ninguna garantía frente a la revelación no autorizada de la información.
- Nivel 1 (*clearing*): Borrado usando mecanismos de sobreescritura del espacio ocupado por los archivos a borrar. La recuperación de la información borrada sólo puede realizarse usando técnicas avanzadas.
- Nivel 2 (*sanitizing*): Borrado seguro. Impide la recuperación de la información borrada incluso utilizando mecanismos avanzados. Algunas de las técnicas que se pueden utilizar para realizar este borrado son: la desmagnetización del soporte; el borrado seguro mediante *firmware* incorporado al soporte físico; la sobreescritura de la información con protocolos que hagan imposible su reconstrucción (generalmente mediante una serie consecutiva de sobreescrituras); o el cifrado de la información con criptografía fuerte y ofuscación de la clave de cifrado empleada.
- Nivel 3: Destrucción física del soporte (destrucción segura). Se realiza por procesos industriales como triturado, incineración, pulverización, fusión de los materiales de que constan los soportes, etc.

En todo caso, se respetarán las previsiones del ENS, en especial para la medida mp.si.5 (borrado y destrucción).

2.5.9.3. Recomendaciones para la elección del nivel destrucción de la información

A fin de determinar el nivel de borrado más adecuado para un caso específico, hemos de tener en cuenta los siguientes parámetros:

- El nivel de confidencialidad de la información que va a destruirse. Dicho nivel será el más elevado de entre los dos siguientes:
  - La categoría del sistema de información según lo establecido en el Anexo I del ENS.
  - El nivel de seguridad de la información según el Reglamento de desarrollo de la LOPD.
- El proceso de borrado va a ser gestionado y realizado por la propia organización (internamente) o, por el contrario, va a ser realizado por una empresa externa en el marco de un contrato de prestación de servicios. En este ámbito, se deben tener en cuenta dos casos concretos:
  - Tendrá la consideración de gestión externa cualquier procedimiento de borrado que se realice en el contexto de servicios en nube cuya infraestructura no sea de gestión privada de la organización.
  - En el caso de la cesión a terceros de la destrucción física de los dispositivos, se recomienda realizar previamente un borrado de nivel 2 sobre su contenido.
- El hecho de si se va a reutilizar o no el soporte de información tras el borrado de la misma.

De acuerdo con estos parámetros, el nivel mínimo de borrado que se recomienda realizar es el que expresa la tabla del anexo VI.

Se recomienda, siempre que sea posible, optar por técnicas de borrado que puedan ser realizadas dentro de la propia organización (tales como: el borrado por *firmware*, la sobreescritura, el cifrado seguro, etc.). De esta manera, se impedirá la entrega de soportes de información a agentes externos, con el consiguiente peligro de ruptura en la cadena de custodia.

En caso de realizar la destrucción a través de la contratación de servicios externos, a la empresa se le debe exigir un certificado de destrucción de los documentos donde conste que la información ya no existe, así como dónde, cuándo y cómo ha sido destruida. Resulta imprescindible dejar constancia de las actividades realizadas, por lo que el certificado sirve para la auditoría y evaluación del cumplimiento de los requisitos acordados. Asimismo, se exigirá que un empleado público fedatario presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados, para firmar la correspondiente acta de eliminación.

2.6. Asignación de Metadatos.

La definición genérica de metadato, según figura en el Esquema Nacional de Interoperabilidad, es “dato que define y describe otros datos". Existen diferentes tipos de metadatos según su aplicación.

Los metadatos constituyen uno de los tres componentes del documento electrónico, junto con el contenido, entendido como el conjunto de datos en que se sustancia la información de un documento electrónico, y con la firma electrónica.

El Artículo 26 de la Ley 39/2015 define:

> 1. *Se entiende por documentos públicos administrativos los válidamente emitidos por los órganos de las Administraciones Públicas. Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia.*
>
> *2. Para ser considerados válidos, los documentos electrónicos administrativos deberán:*
>
> > *a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.*
> >
> > *b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.*
> >
> > *c) Incorporar una referencia temporal del momento en que han sido emitidos.*
> >
> > ***d) Incorporar los metadatos mínimos exigidos.***
> >
> > *e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable.*
>
> *Se considerarán válidos los documentos electrónicos, que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos.*
>
> *3. No requerirán de firma electrónica, los documentos electrónicos emitidos por las Administraciones Públicas que se publiquen con carácter meramente informativo, así como aquellos que no formen parte de un expediente administrativo. En todo caso, será necesario identificar el origen de estos documentos.*

La Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos en su apartado

VII.4 se refiere al Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), que 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 electrónicos. Podrá ser usado como referencia y herramienta de apoyo para la adecuación de cada organización a los requisitos de interoperabilidad en materia de gestión de documentos.

El esquema e-EMGDE establece:

- El modelo conceptual en el que se apoya el modelo de metadatos, sus propiedades y su lógica subyacente.
- La descripción de cada uno de los elementos y subelementos de metadatos, a través de la descripción de cada una de sus características: definición, propósito, obligatoriedad, etc.
- Los esquemas de valores necesarios para cumplimentar los valores de los elementos de metadatos pertinentes.
- Las referencias a las normas utilizadas como base, así como a otras normas de posible utilidad.

El e-EMGDE incluye los metadatos mínimos obligatorios, definidos en las NTI de Documento Electrónico y Expediente electrónico, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos.

Se asignarán a los documentos y expedientes electrónicos los metadatos mínimos obligatorios ENI y, en su caso, los obligatorios para la transferencia, además de los opcionales si se considera oportuno, de conformidad con el perfil de aplicación de metadatos de la organización.

Se garantizarán la disponibilidad e integridad de los metadatos de los documentos y expedientes electrónicos, manteniendo de manera permanente las relaciones entre cada documento o expediente y sus metadatos.

2.6.1. Consideraciones sobre los metadatos mínimos obligatorios

La información necesaria para completar los metadatos mínimos obligatorios de un documento/expediente electrónico deberá generarse durante su captura, es decir, en el momento de su incorporación al SGDE de la organización. No será obligatorio en ese momento que los metadatos sigan la codificación y formato previsto en las correspondientes Normas Técnicas de Interoperabilidad, siempre y cuando puedan transformarse en dicho formato en un momento posterior.

Los metadatos mínimos asociados a un documento o expediente electrónico deberán custodiarse en el repositorio físico utilizado por el SGDE o en otros repositorios que contengan documentación electrónica.

Las diferentes técnicas de almacenamiento de los metadatos contemplan desde el encapsulado, donde el documento se convierte en una entidad que incorpora documento y metadatos, hasta la incrustación de los metadatos como cabecera del documento.

Asimismo, pueden custodiarse en el repositorio físico utilizado por el SGDE de forma separada, siempre y cuando se garantice el mantenimiento de una referencia unívoca entre los documentos y expedientes electrónicos y sus metadatos correspondientes.

Una vez realizada la captura, los metadatos mínimos no podrán ser modificados en ninguna fase posterior, excepto cuando sea necesaria la corrección de errores u omisiones en los valores inicialmente asignados. Por este motivo, el SGDE mantendrá una auditoría de las modificaciones realizadas en los metadatos mínimos de un documento/expediente con posterioridad a su captura, dejando constancia del valor anterior, la fecha y hora de modificación, el motivo justificado y el usuario que la realizó.

El SGDE deberá generar los metadatos mínimos obligatorios con el formato y conforme a la estructura (mediante un esquema XML) establecida en las NTI de Expediente Electrónico y Documento Electrónico, en los casos siguientes:

- Cuando se produzca el intercambio del documento/expediente con otra Administración Pública.
- Cuando el documento/expediente sea puesto a disposición de los ciudadanos por medio de la Sede Electrónica corporativa o de otro canal de comunicación que se establezca.

2.6.2. Consideraciones sobre los metadatos complementarios.

Los metadatos complementarios de documentos y expedientes electrónicos deberán respetar el formato y la nomenclatura indicados en el esquema institucional de metadatos de la organización.

Estos metadatos podrán generarse en el momento de la captura del documento/expediente electrónico o en una fase posterior y podrán modificarse durante la vida administrativa del documento/expediente.

Algunos metadatos complementarios deben ser generados obligatoriamente en el momento de su captura en el SGDE, por ejemplo en el caso de que se trate de documentos esenciales de la organización o documentos y expedientes reservados o con restricciones de acceso, etc.

Cuando se produzca la transferencia del documento o expediente con cambio de custodia al archivo central, intermedio e histórico, con arreglo a los calendarios de conservación, ciertos metadatos complementarios se convierten también en necesarios en el contexto de una correcta política de gestión de documentos y expedientes electrónicos con el fin de garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad.

En aquellos casos en que se han realizado procesos de valoración, dictamen y análisis de acceso, los metadatos relativos a estos procesos deben ser consignados, convirtiéndose en metadatos necesarios e imprescindibles para la materialización de la transferencia física o de responsabilidad de custodia de la serie.

Como en el caso de los metadatos mínimos obligatorios, deberán ser custodiados en el repositorio físico del SGDE formando parte del documento o expediente electrónico o separado de éste, con las mismas garantías respecto a la univocidad entre ambos elementos.

2.7. Documentación

Los procesos expuestos en el apartado 2.5 deben estar documentados. Se tendrán en cuenta las directrices que puedan establecer las autoridades calificadoras y archivísticas competentes, de acuerdo con la

legislación de archivos que sea de aplicación en cada caso.

2.8. Formación

Dado que la implantación de la administración electrónica supone cambios muy importantes con respecto a la gestión administrativa tradicional, anualmente, se incluirán en el Programa de Formación del IVAP (Instituto Valenciano de Administración Pública) actuaciones destinadas a la formación continua y capacitación del personal responsable, tanto de la ejecución y del control de la gestión de los documentos electrónicos como de su tratamiento y conservación en repositorios o archivos electrónicos. Los órganos directivos competentes en materia de archivos y nuevas tecnologías propondrán, de forma conjunta al IVAP, las acciones de formación en materia de gestión de documentos y archivos electrónicos.

Se diseñarán, en concreto, acciones formativas específicas para cada uno de los tipos de actores involucrados en los diferentes procesos de gestión documental contemplados en la presente Política.

Asimismo, se diseñarán acciones formativas encaminadas a difundir el conocimiento de la cultura digital, el documento electrónico, el expediente electrónico y tramitación electrónica en general, partiendo de la base de que sin una comunicación interna y formación adecuadas el conocimiento e implementación de la tramitación electrónica sería inviable.

2.9. Supervisión y auditoría.

Los procesos de gestión de documentos electrónicos, el programa de tratamiento de documentos electrónicos y la presente Política serán objeto de auditorías con una periodicidad de 5 años. Estas auditorías podrán ser abordadas en el contexto de las auditorías del ENS.

Para la realización de estas auditorías se tendrán en cuenta las siguientes normas y estándares internacionales aplicables a las auditorías de gestión documental: ISO 30300 e ISO 15489.

2.10. Gestión de la Política.

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Gestor de la Política identificado en el apartado 2.3.2.

Se promoverá la constitución de una comisión técnica de carácter multidisciplinar, con presencia de los gestores de la Política y de los gestores de procedimiento administrativo, con el objetivo de realizar un seguimiento de la implantación de la PGDE-GV y proponer las revisiones necesarias sobre la misma.

3. PROCEDIMIENTOS INSTRUMENTALES PARA LA GESTIÓN DE DOCUMENTOS

3.1. Protocolo de digitalización de documentos

3.1.1. Definición de digitalización

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.

Se entiende por digitalización certificada o segura el proceso de digitalización mediante el cual el documento obtenido tiene el mismo valor jurídico que el documento original siempre que, además de garantizar la fidelidad, integridad y autenticidad del documento digitalizado, se garantice, también, la preservación del mismo.

3.1.2. Objetivo

El objetivo principal de este protocolo es servir de guía para los procesos de digitalización segura o certificada que se efectúen en el ámbito de la Administración de la Generalitat, con la finalidad de asegurar la autenticidad, la integridad y la preservación de los documentos digitalizados, de impulsar la administración electrónica y de eliminar los documentos en soporte papel cumpliendo la normativa existente al respecto.

Para ello este documento pretende fijar, por una parte, las condiciones técnicas básicas y, por otra, establecer un procedimiento común para el proceso de digitalización de documentos en el ámbito indicado anteriormente y cumpliendo en cualquier caso con la normativa vigente y aplicable en esta materia.

No se incluyen en este protocolo los procesos de digitalización ordinaria, es decir, no certificada, que son aquellos que no garantizan el valor probatorio pleno de la imagen electrónica obtenida.

3.1.3. Protocolo de digitalización de documentos

El protocolo que se describe en el presente apartado parte de la Norma Técnica de Interoperabilidad de Digitalización de Documentos y toma como referencia principal los protocolos de digitalización incluidos en las políticas de gestión de documentos electrónicos de los Ministerios de Hacienda y Administraciones Públicas y de Educación, Cultura y Deporte, así como la experiencia de entidades y organismos que disponen de una práctica consolidada en procesos de digitalización.

3.1.3.1. Directrices generales de digitalización

Los requisitos y criterios que se han de seguir ante procesos de digitalización de documentos constituirán las condiciones mínimas aplicables a cualquier proceso de digitalización que se lleve a cabo en el organismo y deberán ajustarse a lo establecido en el apartado IV de la NTI de digitalización de documentos en cuanto a los siguientes requisitos de la imagen electrónica:

1. *Las imágenes electrónicas aplicarán los formatos establecidos para ficheros de imagen en la Norma Técnica de Interoperabilidad de Catálogo de Estándares.*
2. *El nivel de resolución mínimo para imágenes electrónicas será de 200 píxeles por pulgada, tanto para imágenes obtenidas en blanco y negro, como para color o escala de grises.*

3. *La imagen electrónica será fiel al documento origen, para lo cual:*

   a) Respetará la geometría del documento origen en tamaños y proporciones.

   b) No contendrá caracteres o gráficos que no figurasen en el documento origen.

El proceso de digitalización se llevará a cabo cuando se pretenda aportar al expediente electrónico documentos de naturaleza física, excluyendo aquellos soportes que registren sonido, vídeo o ambos.

Asimismo, es importante, como regla general directamente relacionada con la digitalización, el contenido del artículo 16.2 de la Ley 39/2015:

"*Los documentos presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizados, de acuerdo con lo previsto en el artículo 27 y demás normativa aplicable, por la oficina de asistencia en materia de registros en la que hayan sido presentados para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado, sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización.*"

3.1.3.2. Requisitos técnicos

Sobre la base de los requisitos mínimos de carácter normativo se relacionan una serie de aspectos que han de considerar las unidades responsables del desarrollo de procesos de digitalización. Todos o algunos de estos requisitos, en función del caso, habrán de tenerse en cuenta en procesos de gestión interna o en licitaciones de procesos externalizados.

Estos requisitos tienen que ver con la resolución, profundidad de color y formato de la imagen electrónica obtenida. Como regla general, la digitalización de documentos se llevará a cabo con los siguientes parámetros:

- Se debe contemplar la posibilidad de digitalización a doble cara según las necesidades específicas de cada centro.
- Digitalización con una resolución mínima de 200 ppp (píxeles por pulgada). En caso de que se juzgue necesario para la obtención de una imagen fiel y legible, está resolución podrá ser incrementada.
- Digitalización con la mínima profundidad de color necesaria para cada tipo documental que permita su conservación sin pérdida significativa de información.
- El formato de salida de la imagen digital se corresponderá con alguno de los recogidos en la categoría "Formatos de ficheros - Imagen y/o texto" de la NTI de Catálogo de Estándares. Se recomienda que el formato de salida predeterminado sea PDF o PDF/A (versión 1.4 o superior), a menos que el tratamiento posterior a realizar con el documento haga más aconsejable otro diferente. En el caso de formatos de imagen:
  - JPEG (ISO 15444), al tratarse de un formato con pérdidas degenerativo, solo debe ser utilizado para copias de consulta con valor meramente informativo que requieran un tamaño, en bytes, reducido para su difusión en línea tanto en una intranet como en Internet. Se ha de restringir su uso en documentos de archivo.

- PNG (ISO 15948), como formato de compresión sin pérdidas para imágenes de mapa de bits.
- SVG (W3C), para documentos cartográficos.
- TIFF (ISO 12639), para conservación permanente de documentos de carácter histórico.
- PDF (ISO 32000-1:2008) y PDF/A-1 y A-2 (ISO 19005/1 y 2), en caso de procesos de digitalización para evitar la conservación de papel y para información textual o gráfica de carácter instrumental, así como para facilitar los procesos de firmado y copia auténtica.

- A criterio de la unidad tramitadora, además del proceso de digitalización se contempla la posibilidad de la realización del proceso de reconocimiento óptico de caracteres (OCR en sus siglas en inglés). El documento resultante del procesamiento OCR se tratará como borrador de trabajo, asociado a la imagen digital, de modo que no tendrá la consideración de documento administrativo electrónico (por ejemplo, no se firmará digitalmente). Se aconseja que este proceso se realice de forma simultánea a la obtención de la imagen digital para seleccionar la resolución más adecuada.
- Si procede, para garantizar su legibilidad se puede hacer un proceso de optimización automática de la imagen electrónica, de modo que todo contenido del documento de origen pueda apreciarse y sea válido para su gestión.

El anexo VII incluye una tabla que recopila los requisitos técnicos mínimos recomendados de los documentos digitalizados para su tramitación administrativa.

3.1.3.3. Escenarios de captura

Los escenarios de captura más habituales son los siguientes:

- **En función del agente que efectúa la digitalización:**
  - Digitalización de documentos en soporte físico aportados por el propio ciudadano y entregados en una oficina de registro presencial con ocasión del inicio o tramitación de una solicitud.
  - Documentos en soporte físico digitalizados por un empleado público, durante la tramitación de un procedimiento administrativo, para su incorporación al expediente electrónico asociado.
  - Digitalización masiva de volúmenes elevados de archivos administrativos con expedientes en soporte físico. Se puede diferenciar entre:
    - Digitalización realizada por una unidad administrativa con sus propios medios.
    - Digitalización realizada por un tercer prestador de servicios, por cuenta de una unidad administrativa.
- **En función del momento en el que se efectúa la digitalización:**
  - En tiempo real: en el caso del primer escenario de la clasificación anterior, esta modalidad se realizará si lo permiten los medios técnicos de la oficina de registro. El funcionario digitalizará la documentación en papel aportada para su incorporación a un expediente electrónico y podrá devolver la misma al ciudadano.
  - En diferido: en el caso del primer escenario de la clasificación anterior, el organismo podrá considerar como independientes los procesos de registro y de digitalización. Para ello, una vez recogidos los documentos en formato físico, se generará una carátula para cada uno de los

mismos, de forma que el proceso de digitalización se pueda realizar con posterioridad. Dicha carátula contendrá la información necesaria para la correcta agregación de cada documento al expediente final en la unidad tramitadora.

- En ambas modalidades, los documentos digitalizados se podrán incorporar de forma provisional a un expediente de registro que recopila los documentos con un asiento registral y se transfiere a la unidad administrativa competente para su tramitación.

- **En función del lugar en el que se efectúa la digitalización:**
  - Puntos de digitalización, que habitualmente responden al siguiente perfil:
    - Digitalización inmediata dada la proximidad al usuario, generalmente en oficinas de registro o en puntos de digitalización por planta para la captura electrónica de documentos en papel, registrados en los diferentes puntos de acceso al Registro General.
    - Escáneres de propósito general de sobremesa o equipos multifunción de diferente gama que realizan escaneo, fotocopiado, impresión o envío de fax.
    - Puestos no asistidos por personal especializado.
  - Centros de digitalización, ya sean propios o externalizados, con las siguientes características:
    - Digitalización diferida en el tiempo.
    - Digitalización masiva, por lotes de documentos.
    - Escáneres de medio o alto volumen.
    - Personal especializado.
    - Atención a sus propias necesidades y las de otros.
    - Capacidad, en su caso, para el archivo de los documentos digitalizados.

3.1.3.4. Fases del proceso

Desde el punto de vista del desarrollo del proceso de digitalización documental, podemos distinguir tres grandes bloques diferenciados, cada uno de ellos con sus propias características y tareas, que son la fase de inicio, la fase de digitalización y, por último, la fase de archivo.

- En la primera fase, la de inicio, la documentación tiene que quedar preparada para su digitalización, desde el punto de vista físico, en cuanto a la manipulación, individual o por lotes.

  Cuando el proceso de digitalización se desarrolla en una oficina de registro, la determinación del procedimiento y expediente a los que va a quedar vinculado el documento una vez digitalizado corresponderá a la unidad tramitadora de destino.

- En la segunda fase, la de digitalización propiamente dicha, como resultado se obtendrán documentos ENI conformados, es decir, con contenido, firma electrónica y metadatos mínimos obligatorios y complementarios (metadatos complementarios asociados al procedimiento de digitalización). Este resultado debe observar, además, el esquema de metadatos para la gestión del documento electrónico de la organización (e-EMGDE), que incluirá los metadatos mínimos obligatorios que establecen las NTI de documento electrónico, copiado auténtico y conversión y

digitalización de documentos electrónicos.

El proceso de digitalización de documentos deberá, además, someterse a un control de calidad que permita detectar errores en cuanto al número o aspecto de las imágenes resultantes, de manera que se cumpla lo establecido en la NTI de Digitalización de Documentos en cuanto a los requisitos de la imagen electrónica.

- La tercera y última fase, la de archivo**,** tendrá que determinar el destino de los documentos en papel que han sido digitalizados para su incorporación como documentos electrónicos a su correspondiente expediente electrónico, ya sea este su archivo físico o su destrucción reglada.

3.1.3.4.1. Primera fase. Iniciación

En esta fase se deberán identificar los documentos que se desea digitalizar. Será necesario, también, determinar cuál va a ser el escenario de digitalización, puesto que el proceso se ajustará a uno u otro entorno y la asignación de metadatos a los documentos electrónicos resultantes se hará, según el caso, de forma manual o automática.

En cualquier caso, la digitalización de los documentos irá precedida de una manipulación y preparación previa, así como de la declaración de los datos identificativos y descriptivos de los mismos en forma de metadatos.

Esta fase inicial, fundamentalmente dedicada a la preparación de los documentos a digitalizar, se describe en el anexo IX de este documento.

3.1.3.4.2. Segunda fase. Digitalización

Una vez finalizada la fase anterior, los documentos ya se encuentran preparados y debidamente organizados y clasificados en la ubicación definitiva de digitalización.

Se deben adoptar las medidas necesarias para que el proceso de digitalización se realice de acuerdo con los requisitos técnicos recomendados anteriormente relativos al formato del fichero a obtener, resolución, pro - fundidad de bit, color, etc., en función del tipo de documento origen.

También se determinará el nivel de agrupamiento multipágina/monopágina del resultado, es decir, si se va a crear un único fichero con una o varias páginas por cada documento original (multipágina) o varios ficheros, cada uno con una página (monopágina). Se recomienda que el nivel de agrupamiento sea multipágina, de forma que cada fichero se corresponda con un documento completo de una o más páginas.

3.1.3.4.2.1. Asignación de metadatos

Como se ha indicado anteriormente y siempre que el formato de salida lo admita, se añadirán en el momento de la digitalización, a los documentos electrónicos resultantes, los metadatos complementarios del procedimiento de digitalización y los metadatos mínimos obligatorios que contemple el esquema de metadatos e-EMGDE-GV de la organización.

La incorporación de los metadatos citados al sistema de gestión de documentos electrónicos o a otro sistema de soporte que utilice la organización debe realizarse, siempre que sea posible, de forma automática por medio de las funcionalidades ofrecidas por el propio SGDE u otro sistema que opere en una capa superior. En los casos y/o situaciones en los que la asignación automática de metadatos no sea posible total o parcialmente, éstos se incluirán manualmente utilizando el mismo tipo de funcionalidades y en la etapa más temprana posible del ciclo de vida del documento electrónico.

Se valorará el empleo del sistema de carátulas con código de barras o similar, mediante el que la asignación de metadatos se haga con carácter previo a la digitalización de los documentos, como método para garantizar la completitud en la asignación de los metadatos obligatorios y complementarios durante la fase de creación y captura del documento electrónico.

3.1.3.4.2.2. Firma de los documentos electrónicos digitalizados

Para conformar un documento ENI a partir de una imagen digital, deberán añadirse a la misma los metadatos de firma establecidos en las NTI de documento electrónico y de digitalización de documentos electrónicos y, además, deberá ser firmado electrónicamente durante el proceso de digitalización mediante cualquiera de los sistemas de firma admitido por la Ley 11/2007 [12] -Ley 39/2015 a partir del 2 octubre de 2016- y el Decreto 220/2014 de la Generalitat.

La firma electrónica se aplicará al fichero imagen obtenido y, aunque los metadatos no estén incrustados en la imagen sino, por ejemplo, vinculados a la misma a través del SGDE, de aplicaciones de gestión o de archivos de texto, el hecho de que estos metadatos no estén firmados no invalida la imagen puesto que constituyen una capa independiente. Tales metadatos darán cuenta del contexto y existencia de la firma electrónica que, a su vez, valida la imagen.

3.1.3.4.2.3. Validez de los documentos electrónicos obtenidos en el proceso de digitalización

Un documento original es aquel que se conserva tal y como fue emitido por su autor, tanto en sus características externas como internas. Una copia es el resultado de la reproducción de un documento. Desde el punto de vista legal hay dos tipos de copia:

- Copia simple, aquella que no tiene valor probatorio y se establece para disponer de una copia del documento original.
- Copia auténtica, aquella que tiene la misma validez y eficacia que el documento original.

Respecto de la validez de los documentos obtenidos como copias electrónicas auténticas y/o su consideración como copias electrónicas compulsadas, se estará a lo establecido en los artículos 60 y 64 del Decreto 220/2014 de la Generalitat, en la NTI de copiado auténtico y conversión, así como en el artículo 27 de la Ley 39/2015 que entrará en vigor a partir del 2 octubre de 2016.

3.1.3.4.2.4. Control de calidad

Se efectuarán controles de calidad para asegurar que el proceso de digitalización se ha efectuado correctamente. Estos controles consisten en verificar que tanto la imagen digital como los datos significativos obtenidos en el proceso de digitalización son fieles al documento original en papel y cumplen con unos requisitos mínimos necesarios de calidad y fidelidad respecto al original.

El control de calidad incluirá, como mínimo, las siguientes verificaciones:

- Cumplimiento de los requisitos mínimos de las imágenes digitalizadas.
- Completitud de los metadatos introducidos.
- Comprobar el número de hojas digitalizadas respecto al documento origen, en aquellos casos en que se haya efectuado el recuento exacto de hojas del documento origen.
- Cotejar el documento electrónico con el documento origen en papel, en una muestra de los

12 Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre

documentos digitalizados. Se efectuarán los siguientes controles:

- Corrección de las imágenes obtenidas en cuanto a calidad de la imagen o en cuanto a criterios técnicos:
  - Resolución adecuada al tipo documental.
  - Color adecuado al tipo documental.
  - Formato adecuado al tipo documental.
  - Alineación correcta de la imagen.
- Corrección de las imágenes obtenidas en cuanto a fidelidad con el original:
  - Digitalización de todas las páginas del documento.
  - Digitalización sin inclusión de información que no aparece en el original.
  - Visualización y legibilidad de la imagen.

Es conveniente prever la realización de auditorías periódicas del proceso para asegurar la calidad del procedimiento a lo largo del tiempo.

En los casos en que se realice una digitalización masiva, estos controles se realizarán a partir de una muestra estadísticamente representativa. Tal muestreo debe realizarse necesariamente para la correcta recepción de trabajos de digitalización masiva realizados por terceros por cuenta de la Administración.

3.1.3.4.3. Tercera fase. Archivo

La última de las fases es la que se corresponde con el tratamiento de los documentos físicos tras comprobar que el proceso de digitalización ha finalizado correctamente.

Se deberá, en primer lugar, determinar cuáles de los documentos digitalizados deben ser archivados físicamente y cuáles no, bien porque se digitalicen en el momento del registro y sean devueltos al ciudadano, bien porque se haya valorado la oportunidad de su destrucción.

La determinación del archivado físico de documentos puede deberse, en términos generales, a dos causas:

- La obligación de que en los procedimientos obren los documentos originales, en cuyo caso las unidades responsables de la tramitación de los mismos deberán indicar en qué caso es preceptiva la aportación de originales, para así garantizar su custodia una vez digitalizados.
- Que lo que se haya incorporado al procedimiento electrónico sea un documento electrónico creado a partir de la digitalización de una fotocopia. En este caso, habrá que actuar siguiendo las indicaciones que figuran en el anexo IX (preparación de la documentación a digitalizar) respecto al tratamiento de documentos de características especiales que deben ser fotocopiados con carácter previo a su digitalización.

En caso de que, por el contrario, se juzgue oportuna la destrucción de los documentos en papel digitalizados, ésta se realizará de acuerdo a la PGDE-GV y al artículo 62 del Decreto 220/2014, siempre cumpliendo las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establezca el Esquema Nacional de Seguridad.

4. REFERENCIAS

4.1. Normativa estatal

- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- 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.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- 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.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Modificada en virtud de Ley 18/2015, de 9 de julio.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente.
- Real Decreto Legislativo 1/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Catastro Inmobiliario.
- Ley 58/2003, de 17 de diciembre, General Tributaria.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

- Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 12/1989, de 9 de mayo de 1989, de la Función Estadística Pública.
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 13/1985, de 25 de junio, del Patrimonio Histórico Español.
- Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.
- Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, intimidad personal y familiar y a la propia imagen.
- Ley 9/1968, de 5 de abril, sobre secretos oficiales.

4.1.1. Normas Técnicas de Interoperabilidad

- Resolución de 19 de febrero de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Reutilización de recursos de la información.
- Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares.
- 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 Relación de modelos de datos.
- 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 Protocolos de intermediación de datos.
- 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.
- 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 Documentos.
- 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.
- 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.
- 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 Política de Firma Electrónica y de certificados de la Administración.
- 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 Procedimientos de copiado auténtico y conversión entre documentos electrónicos.

- 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 Modelo de Datos para el Intercambio de asientos entre las entidades registrales.
- 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 requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas.

4.1.2. Guías Técnicas de Interoperabilidad

- Esquema de metadatos para la Gestión del Documento Electrónico (e-EMGDE).
- Guía de aplicación de la NTI de Política de Gestión de Documentos Electrónicos.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Catálogo de estándares.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Documento Electrónico.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- Guía de aplicación de la Norma Técnica de Política de Firma Electrónica y de certificados de la Administración.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Relación de modelos de datos.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: SICRES 3.0.
- Guía de aplicación de la Norma Técnica de Interoperabilidad de Reutilización de recursos de información.
- Reutilización de activos. Guía de publicación y licenciamiento de activos.

4.2. Normativa autonómica

- Resolución de 5 de mayo de 2015, del secretario autonómico de Administración Pública, por la que se dictan las directrices de funcionamiento y se aprueba el manual de instrucciones que será de obligado cumplimiento para todas las oficinas de registro de la Generalitat, incluidas en el ámbito de aplicación del Decreto 191/2014, de 14 de noviembre, del Consell.
- Ley 2/2015, de 2 de abril, de la Generalitat, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana.
- Ley 7/2014, de 22 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat.
- Decreto 220/2014, de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.
- Orden 19/2013, de 3 de diciembre, de la Consellería de Hacienda y Administración Pública, por la que se establece las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat.
- Orden 7/2012, de 27 de septiembre, de la Conselleria de Hacienda y Administración Pública, por la que se regula el catálogo de procedimientos administrativos de la administración de la Generalitat y su sector público.
- Decreto 138/2012, de 14 de septiembre, del Consell, por el que se regulan los Servicios de Atención e Información al Paciente (SAIP).
- Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat.
- Decreto 130/2012, 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat.
- Orden 3/2011, de 15 de marzo, de la Conselleria de Cultura y Deporte, por la que se aprueba el Reglamento de Composición, Organización y Funcionamiento del Consejo Asesor de Archivos de la Comunitat Valenciana.
- Orden 40/2010, de 11 de noviembre, de la Conselleria de Economía, Hacienda y Empleo, por la que se modifica el anexo del Decreto 18/2004, de 13 de febrero, del Consell de la Generalitat, de creación del Registro Telemático de la Generalitat y regulación de las notificaciones telemáticas de la Generalitat, actualmente denominado Registro Electrónico de la Generalitat.
- Decreto 165/2010, de 8 de octubre, del Consell, por el que se establecen medidas de simplificación y de reducción de cargas administrativas en los procedimientos gestionados por la administración de la Generalitat y su sector público.
- Resolución de 27 de agosto de 2010, de la consellera de Justicia y Administraciones Públicas, por la que se aprueba la Carta de Servicios de la Guía Prop Electrónica.
- Decreto 87/2010, de 21 de mayo, del Consell, por el que se establecen las condiciones técnicas y normativas para el uso de la Plataforma de Facturación Electrónica de la Generalitat, Ge-factura.
- Orden 17/2010, de 13 de mayo, de la Conselleria de Economía, Hacienda y Empleo, por la que se

establecen las condiciones generales del intercambio electrónico de datos en el ámbito de la conselleria.

- Decreto 62/2010, de 16 de abril, del Consell, por el que se establecen los instrumentos generales del sistema para la modernización y mejora de la calidad de los servicios públicos de los entes, organismos y entidades del sector público dependientes de la Generalitat.
- Orden 4/2010, de 19 de febrero, de la Conselleria de Infraestructuras y Transporte, por la que se regula la entrega de proyectos de obra en formato digital en la Conselleria de Infraestructuras y Transporte.
- Orden de 6 de julio de 2009, de la conselleria de Economía, Hacienda y Empleo, por la que se aprueba el procedimiento de notificación electrónica del contenido de los contratos de trabajo y sus copias básicas en el ámbito de la Comunitat Valenciana.
- Orden de 17 de septiembre de 2008, de la Conselleria de Economía, Hacienda y Empleo, por la que se aprueba la aplicación de la Plataforma de Contratación de la Generalitat.
- Decreto 189/2005, de 2 de diciembre, del Consell de la Generalitat, por el que se regula la Junta Calificadora de Documentos Administrativos y el procedimiento de valoración, conservación y eliminación del patrimonio documental de los archivos públicos.
- Orden de 14 de julio de 2005, del conseller de Infraestructuras y Transporte, por la que se establecen las condiciones generales y el procedimiento para la aplicación de los estándares definidos para el uso de la firma electrónica avanzada mediante Rubric@CV.
- Ley 3/2005, de 15 de junio, de la Generalitat, de Archivos.
- Orden de 6 de junio de 2005, de la Conselleria de Infraestructuras y Transporte por la que se establecen las condiciones generales y se aprueba la Plataforma corporativa para la Tramitación y Notificación Telemática de la Generalitat Valenciana – Generalitat en Red.
- Resolución de 15 de abril de 2004, de la secretaría autonómica de Telecomunicaciones y Sociedad de la Información, por la que se establecen las medidas técnicas y organizativas necesarias que, con carácter general, habrán de reunir las unidades registrales telemáticas y todos los procedimientos administrativos para que sean susceptibles de tramitación telemática a través del Registro Telemático de la Generalitat Valenciana.
- Ley 4/1998, de 11 de junio, del Patrimonio Cultural Valenciano.

4.3. Otros documentos de interés

- Directorio Común de Unidades Orgánicas y Oficinas. Modelo de Codificación y Manual de Atributos de Información.
- Sistema de Información Administrativa.
- Documento ISO/TC 46/SC 11 N800R1, relativo a “orientaciones sobre la elaboración de un esquema de metadatos”, y que constituye un desarrollo de la norma ISO 23081
- Criterios generales para la valoración de los documentos de la Administración General del Estado. Documento aprobado por la Comisión Superior Calificadora de Documentos Administrativos, en sesión de 27 de noviembre de 2003.

- Especificaciones de MoReq-2
- Guía de Comunicación Digital para la Administración del Estado.
- Norma UNE-ISO 15489-1:2006. Información y documentación. Gestión de documentos. Parte 1: Generalidades.
- Norma UNE-ISO 23081-1:2008. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 1: Principios.
- Norma UNE-ISO 23081-2:2011. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Elementos de implementación y conceptuales.
- Norma UNE-ISO 30300:2011. Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario.
- Norma UNE-ISO 30301:2011. Información y documentación. Sistemas de gestión para los documentos. Requisitos.
- Modelo de Política de Gestión de Documentos Electrónicos del Ministerio de Hacienda y Administraciones Públicas.
- NARA's Open government plan 2012-2014.
- Política de Gestión de Documentos del Ministerio de Hacienda y Administraciones Públicas.
- Requisitos del Modelo para la Gestión de Archivos Electrónicos.
- Norma UNE-ISO 14641-1:2015 Archivo electrónico. Parte 1: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital.
- Norma UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.
- Política de gestión de documentos electrónicos del MINHAP.
- Política de gestión del documento electrónico del MECD.
- Política de gestión de documentos electrónicos de la Administración Pública de la comunidad autónoma de Canarias.

5. SIGLAS Y ACRÓNIMOS

- E-EMGDE: Esquema de Metadatos para la Gestión del Documento Electrónico
- ENI: Esquema Nacional de Interoperabilidad
- ENS: Esquema Nacional de Seguridad
- JCDA: Junta Calificadora de Documentos Administrativos
- LTAIBG: Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno
- MoReq: Model Requirements for the Management of Electronic Records / Modelo de Requisitos para la Gestión de Registros Electrónicos
- PGDE-GV: Política de Gestión de Documentos Electrónicos de la GVA
- SGDEA: Sistemas de Gestión de Documentos Electrónicos de Archivo.