Política de gestión de documentos electrónicos del Ministerio de Defensa

MINISTERIO DE DEFENSA

Política de gestión de documentos electrónicos del Ministerio de Defensa

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

http://publicaciones.defensa.gob.es/

PUBLICACIÓN DE ÁMBITO INTERNO

Fecha de edición: marzo, 2017

Imprime: Ministerio de Defensa

En esta edición se ha utilizado papel 100% reciclado libre de cloro.

Orden Ministerial 5/2017, de 9 de febrero, por la que se aprueba la Política de gestión de documentos electrónicos del Ministerio de Defensa

La recientemente derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, marcó un punto de inflexión en la utilización de las denominadas tecnologías de la información y las comunicaciones en las relaciones de las Administraciones Públicas con los ciudadanos y en asegurar la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por dichas Administraciones públicas entre sí.

El 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, permitió la elaboración, entre otras, de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos, aprobada por Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, en la que se establecen los conceptos relacionados con el desarrollo de políticas de gestión de documentos electrónicos, se identifican los procesos de la gestión de documentos en el marco de la administración electrónica y se establecen los principios necesarios para el desarrollo y aplicación de políticas de gestión de documentos electrónicos por parte de todos los órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla.

Por otra parte, la Agenda Digital aprobada en Consejo de Ministros en febrero de 2013, la Ley 19/2013 de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y 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, han configurado la estrategia de las administraciones públicas en el ámbito digital y de las comunicaciones y han creado un conjunto normativo con el que se ha pretendido trasladar los beneficios de las nuevas tecnologías a los ciudadanos y a las Administraciones públicas y lograr de esa forma una mayor eficacia en la gestión, garantizando la seguridad en las comunicaciones.

También, la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, responsables de la derogación de la inicialmente mencionada Ley 11/2007, de 22 de junio, ha permitido establecer que el uso de medios electrónicos tiene que constituir el medio preferente en las relaciones de las Administraciones públicas con los ciudadanos y de aquellas entre sí y pone de relieve que una administración sin papel, basada en un funcionamiento íntegramente electrónico, sirve mejor a los principios de eficacia y eficiencia al ahorrar costes a los ciudadanos y a las Administraciones públicas, y refuerza las garantías de los interesados.

Por otra parte, y de manera casi simultánea a la publicación de las mencionadas Leyes 39/2015 y 40/2015, se ha definido el marco global para avanzar en la transformación de la Administración, estableciendo sus principios rectores, los objetivos y las acciones para alcanzarlos, así como los hitos para su desarrollo gradual, plasmándolo en la elaboración del Plan de Transformación Digital de la Administración General del Estado y sus Organismos Públicos, aprobado en Consejo de Ministros el 2 de octubre de 2015, que orienta al desarrollo de planes de acción para la transformación digital de cada departamento, que deben converger con los principios, objetivos y líneas de acción de la estrategia TIC de la Administración General del Estado, salvaguardando las características particulares en cada ámbito y, en el caso que nos ocupa, en el ámbito de la defensa nacional.

El mencionado Plan de Transformación Digital incluye una primera línea de acción que se centra en la transformación de los procesos de gestión internos de las unidades administrativas en electrónicos y, entre las medidas para lograrlo, señala la necesidad de elaborar una Política de gestión de documentos electrónicos que asegure su aceptación en las distintas unidades, que contemple la organización documental, la clasificación de la información y la aplicación de estándares para facilitar el intercambio por medios electrónicos, así como su archivo.

En base a todas estas circunstancias, en el Departamento se ha elaborado la Política de Gestión de los Documentos Electrónicos del Ministerio de Defensa, cuyo texto ha sido aprobado en el ámbito de la Comisión Permanente de la Comisión Ministerial de Administración Digital en su reunión del pasado 22 de julio de 2016 y que ha contado con el posterior visto bueno de la Dirección de Tecnologías de la Información y Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.

Por todo lo anterior,

DISPONGO:

Artículo único. *Aprobación de la Política de gestión de documentos electrónicos del Ministerio de Defensa*.

Se aprueba la Política de gestión de documentos electrónicos del Ministerio de Defensa, cuyo texto se inserta a continuación.

Disposición final única. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Ministerio de Defensa».

Madrid, 9 de febrero de 2017

MARÍA DOLORES DE COSPEDAL GARCÍA

ÍNDICE DE CONTENIDOS

Página

Introducción 13

1. Definiciones y alcance 17

1.1. QUÉ ES Y QUÉ OBJETIVOS SE PERSIGUEN CON LA PGDE-MINISDEF 17

1.2. QUÉ SON DOCUMENTOS ELECTRÓNICOS 18

1.2.1. Definición 18

1.2.2. Ciclo de vida de los documentos electrónicos 19

1.3. DIRECTRICES DE LA PGDE-MINISDEF 19

1.4. ÁMBITO DE APLICACIÓN 21

1.5. RIESGOS DERIVADOS DEL INCUMPLIMIENTO DE ESTA POLÍTICA. 21

2. Marco de la PGDE-MINISDEF 23

2.1. ACTORES Y RESPONSABILIDADES 23

2.1.1. Alta Dirección 23

2.1.2. Nivel corporativo 24

2.1.3. Nivel específico 28

2.2. PLANIFICACIÓN 30

2.3. DESARROLLO NORMATIVO Y DOCUMENTACIÓN 31

2.4. ACTUALIZACIÓN DE LA POLÍTICA 32

2.5. FORMACIÓN, DIFUSIÓN Y APOYO 32

2.6. SUPERVISIÓN Y AUDITORÍA 34

2.7. OPERACIÓN DE LA GESTIÓN DOCUMENTAL Y PROGRAMA DE TRATAMIENTO DE LOS DOCUMENTOS 35

Página

3. Esquema de metadatos y su aplicación a los procesos de gestión de los documentos electrónicos 39

3.1. CONCEPTO Y PROPÓSITO DE LOS METADATOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS 39

3.2. ESQUEMA DE METADATOS DEL MINISTERIO DE DEFENSA 40

3.3. ENFOQUE DE IMPLEMENTACIÓN DE LOS METADATOS 41

3.4. APLICACIÓN DE LOS METADATOS EN LA OPERACIÓN DE LOS PROCESOS DOCUMENTALES 42

4. Procesos de creación y captura de documentos electrónicos 45

4.1. IDENTIFICACIÓN Y ANÁLISIS DOCUMENTAL 45

4.2. CREACIÓN DE DOCUMENTOS 47

4.3. CAPTURA DE DOCUMENTOS 48

4.4. REGISTRO ELECTRÓNICO 51

4.4.1. Digitalización en el punto de registro 53

5. Procesos de clasificación documental y descripción 55

5.1. CONCEPTO Y PROPÓSITO DE LA CLASIFICACIÓN DOCUMENTAL 55

5.2. INSTRUMENTOS DE CLASIFICACIÓN 56

5.3. NIVELES DE AGRUPACIÓN DOCUMENTAL 57

5.4. APLICACIÓN DE LA CLASIFICACIÓN DOCUMENTAL 59

5.5. DESCRIPCIÓN 60

6. Procesos de calificación, conservación, transferencia y eliminación 63

6.1. CALIFICACIÓN 63

6.1.1. Concepto y propósito de la calificación 63

6.1.2. Documentos esenciales 63

6.1.3. Valoración y dictamen 64

6.2. CONSERVACIÓN 68

6.3. TRANSFERENCIA 70

6.4. DESTRUCCIÓN O ELIMINACIÓN 73

7. Acceso 77

7.1. ACCESO A LOS DOCUMENTOS ELECTRÓNICOS 77

7.2. RÉGIMEN DE ACCESO 78

7.2.1. Categorías de acceso 78

7.2.2. Documentos electrónicos no clasificados 80

7.2.3. Documentos electrónicos clasificados 81

7.3. APLICACIÓN DE LAS CONDICIONES DE ACCESO 82

8. Trazabilidad 87

Página

9. Identificación y período de validez de la PGDE-MINISDEF 89
9.1. PERÍODO DE VALIDEZ 89
9.2. IDENTIFICADOR DEL GESTOR DE LA POLÍTICA 90

10. Referencias 91
10.1. LEGISLACIÓN Y NORMATIVA 91
10.1.1. Ministerio de Defensa 91
10.1.2. Otras referencias 93
10.2. NORMAS TÉCNICAS DE INTEROPERABILIDAD Y GUÍAS TÉCNICAS .. 97
10.3. DOCUMENTOS DE REFERENCIA 99
10.3.1. Ministerio de Defensa 99
10.3.2. Estándares ISO 100
10.3.3. Otras referencias 101

11. Glosario 105
11.1. TÉRMINOS 105
11.2. ACRÓNIMOS 114

ANEXOS

ANEXO 1. Procedimiento instrumental para la expedición de copias electrónicas auténticas 119
CARACTERÍSTICAS DE LA COPIA ELECTRÓNICA AUTÉNTICA 120
CARACTERÍSTICAS DE LA COPIA ELECTRÓNICA AUTÉNTICA CON CAMBIO DE FORMATO 121
COPIA ELECTRÓNICA PARCIAL AUTÉNTICA 122
COPIA ELECTRÓNICA AUTÉNTICA DE DOCUMENTO ELECTRÓNICO PÚBLICO ADMINISTRATIVO 122
COPIA ELECTRÓNICA AUTÉNTICA DE DOCUMENTOS EN SOPORTE NO ELECTRÓNICO 123
COPIA EN PAPEL AUTÉNTICA DE DOCUMENTOS ADMINISTRATIVOS ELECTRÓNICOS 123
DOCUMENTOS APORTADOS POR EL CIUDADANO 124
DESTRUCCIÓN DE DOCUMENTOS EN SOPORTE NO ELECTRÓNICO 125

ANEXO 2. Control del cumplimiento del ENI en materia de gestión de documentos electrónicos 127

ANEXO 3. Consideraciones para el desarrollo del esquema de metadatos del Ministerio de Defensa 133
ESQUEMA DE METADATOS Y PERFILES DE APLICACIÓN 133
MODELO DE IMPLEMENTACIÓN 136
TABLA DE METADATOS DE REFERENCIA PARA EL E-EEMDEF 138

Página

ANEXO 4. Esquema funcional para el desarrollo del cuadro de clasificación documental de los documentos electrónicos 145

ANEXO 5. Medidas para la preservación a largo plazo 149

CONSERVACIÓN DE LOS DOCUMENTOS ELECTRÓNICOS 149

PRINCIPIOS A APLICAR EN LOS SISTEMAS QUE CONTIENEN INFORMACIÓN DE VALOR PERMANENTE 151

GRUPOS DE RIESGO Y MEDIDAS GENERALES DE CONSERVACIÓN 152

FORMATOS DE ARCHIVO PARA LA CONSERVACIÓN A LARGO PLAZO 163

Conjuntos de datos (Data sets) 164

Texto 165

Imágenes fijas 166

Imágenes en movimiento 167

Sonido 168

Geoespacial 169

Archivo web 169

EQUIVALENCIA ENTRE LOS METADATOS E-EMGDE Y PREMIS 170

ANEXO 6. Metadatos y tablas de valores de referencia relativos al acceso 177

METADATOS E-EMGDE RELATIVOS AL ACCESO Y SEGURIDAD 177

TABLA DE CODIFICACIÓN DE LAS RESTRICCIONES DE ACCESO 178

TABLA DE RÉGIMEN JURÍDICO DE ACCESO ESPECÍFICO 178

TABLA DE NIVELES DE SENSIBILIDAD DE DATOS DE CARÁCTER PERSONAL 179

VALORES ESPECÍFICOS PARA EL ÁMBITO DE LA DEFENSA EN EL E-EMMDEF 180

Introducción

La Agenda Digital aprobada en Consejo de Ministros en febrero de 2013, la Ley 19/2013 de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIP) y la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (LRISP) modificada por la Ley 18/2015, de 9 de julio, configuran la estrategia de las administraciones públicas en el ámbito digital y de las comunicaciones. Con este conjunto normativo se pretende trasladar los beneficios de las nuevas tecnologías a los ciudadanos y a la administración pública y lograr una mayor eficacia en la gestión, garantizando la seguridad en las comunicaciones.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC) y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) establecen que el uso de medios electrónicos tiene que constituir el medio preferente en las relaciones de las administraciones con los ciudadanos y de aquellas entre sí y ponen de relieve que una administración sin papel, basada en un funcionamiento íntegramente electrónico, sirve mejor a los principios de eficacia y eficiencia al ahorrar costes a ciudadanos y administraciones públicas, y refuerza las garantías de los interesados.

En concreto la LPAC se refiere, entre otras, a cuestiones que afectan a los documentos y expedientes electrónicos tales como

los registros, la emisión de documentos por las administraciones públicas, la validez y eficacia de las copias realizadas por las administraciones; los documentos aportados por los interesados, y el archivo de documentos, de forma que cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados.

Además, la LRJSP aborda, entre otras cuestiones, los sistemas de identificación electrónica, la firma electrónica del personal al servicio de las administraciones, la sede electrónica, el intercambio de datos en entornos cerrados de comunicación, la actuación administrativa automatizada, la gestión compartida de los servicios comunes, la aplicación del Esquema Nacional de Interoperabilidad (ENI) y del Esquema Nacional de Seguridad (ENS), la reutilización de sistemas y aplicaciones de propiedad de la Administración y la transferencia de tecnología entre administraciones.

El Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, obliga al desarrollo de planes de acción para la transformación digital de cada departamento, que deben converger con los principios, objetivos y líneas de acción de la estrategia TIC de la Administración General del Estado (AGE), salvaguardando las características particulares en cada ámbito y en concreto en el ámbito de la defensa nacional.

El Plan de Transformación Digital de la AGE y sus Organismos Públicos, aprobado en Consejo de Ministros el 2 de octubre de 2015, constituye el marco global para avanzar en la transformación de la Administración, estableciendo sus principios rectores, los objetivos y las acciones para alcanzarlos, así como los hitos para su desarrollo gradual. La línea de acción 1, se centra en la transformación de los procesos de gestión internos de las unidades administrativas en electrónicos y, entre las medidas para lograrlo, señala la necesidad de elaborar una política de gestión de documentos electrónicos que asegure su aceptación en las distintas unidades, que contemple la organización documental, la clasificación de la información y la aplicación de estándares para facilitar el intercambio por medios electrónicos, así

como su archivo. Igualmente, la Línea 2 desarrolla el puesto de trabajo digital, plantea proveer a los empleados públicos, que participen en el sistema de trabajo, de los medios materiales suficientes para el correcto desempeño de sus funciones, garantizando pleno acceso a la información necesaria y las herramientas colaborativas precisas.

El Ministerio de Defensa inició esta área de actuación con el Plan Director de Sistemas de Información y Telecomunicaciones definido en la Orden DEF/315/2002, de 14 de febrero, por la que se aprueba el Plan Director de Sistemas de Información y Telecomunicaciones y se establece, para su dirección, gestión y seguimiento, el Comisionado del Plan, derogada por la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa. En ella se enmarca la presente Política de Gestión de Documentos Electrónicos en cumplimiento de la Disposición Adicional Primera, h), del 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 y de la 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 –en adelante NTI– de Política de Gestión de Documentos Electrónicos.

La Política de Gestión de Documentos Electrónicos se alinea con la Política de Seguridad de la Información del Ministerio de Defensa y sus normas derivadas, y se integra en el Sistema Archivístico de la Defensa (SAD), manteniendo de este modo la coherencia en la gestión y archivo de los documentos independientemente de su soporte.

Para su elaboración se han tenido en cuenta los contenidos y criterios establecidos en las Normas Técnicas de Interoperabilidad (NTI) y sus guías de aplicación, tomando como punto de partida el modelo de Política de Gestión de Documentos Electrónicos del Ministerio de Hacienda y Administraciones Públicas y el del Ministerio de Educación, Cultura y Deporte, así como las políticas desarrolladas al efecto por la OTAN y otros organismos de Defensa de referencia.

El presente documento de Política de Gestión de Documentos Electrónicos del Ministerio de Defensa se estructura en 11 apartados y 6 anexos documentales.

En el Apartado 1 se establece el ámbito y alcance de la Política de Gestión de Documentos Electrónicos del Ministerio de Defensa –en adelante PGDE-MINISDEF–. Se definen los conceptos necesarios para entender y aplicar la política, se exponen los principios que el Departamento debe cumplir, el ámbito de aplicación y los riesgos derivados del incumplimiento.

El Apartado 2 describe el marco de aplicación necesario para una gestión sistemática de los documentos electrónicos y define los actores y el esquema de responsabilidades, la planificación, la documentación, la formación y difusión, la supervisión y auditoría y el programa de tratamiento de los documentos electrónicos.

A partir del apartado 3 se contienen las directrices de carácter operativo que afectan a los procesos de gestión de documentos electrónicos.

En primer lugar, se desarrollan las previsiones respecto al esquema de metadatos que es el elemento esencial que posibilita la gestión de los documentos en el entorno electrónico y garantiza la interoperabilidad.

En segundo lugar, se desarrollan los procesos de gestión documental que se han dividido en tres agrupaciones conceptuales: creación y captura (apartado 4), clasificación y descripción (apartado 5) y calificación, conservación, transferencia y eliminación (apartado 6).

El apartado 7 contiene los aspectos relacionados con las condiciones de acceso bajo los principios que establece la legislación vigente y el apartado 8 la trazabilidad de las acciones realizadas con la documentación en soporte electrónico.

Los apartados 9 a 11 contienen los datos de identificación de esta política, las referencias empleadas y un glosario de términos.

Por último, la PGDE-MINISDEF se acompaña de una serie de anexos que desarrollan a nivel específico diversos aspectos del cuerpo central.

1. Definiciones y alcance

1.1. QUÉ ES Y QUÉ OBJETIVOS SE PERSIGUEN CON LA PGDE-MINISDEF

La presente política establece las directrices y el marco de actuación para la gestión de los documentos electrónicos del Departamento, con objeto de garantizar su integridad, disponibilidad, confidencialidad y conservación y sustentar la eficiente y efectiva ejecución de los procesos y procedimientos del Ministerio de Defensa por medios electrónicos.

Los principales objetivos que se persiguen con la aplicación de esta política son:

a) Documentar las decisiones, acciones y operaciones del Ministerio de Defensa.
b) Facilitar la planificación, la toma de decisiones y apoyar la formulación de políticas.
c) Proteger los intereses de los ciudadanos y la administración.
d) Proporcionar medios para la rendición de cuentas.
e) Preservar la memoria del Departamento.

Se aplicará a los documentos electrónicos del Ministerio de Defensa y, en lo que proceda, a las situaciones híbridas ya existentes o que se produzcan durante el periodo de transformación digital.

1.2. QUÉ SON DOCUMENTOS ELECTRÓNICOS

1.2.1. Definición

Se define documento como toda información creada, recibida y conservada como evidencia y como activo por el Ministerio de Defensa en el desarrollo de sus actividades o en virtud de sus obligaciones legales. Los documentos, en cualquier soporte, son la evidencia oficial de las acciones y decisiones del Departamento y forman parte de su patrimonio documental.

El artículo 26 de la LPAC establece que «*las Administraciones Públicas emitirán los documentos administrativos, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia*» y define los requisitos que estos deben cumplir para que se consideren documentos electrónicos válidos*:*

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.

Los documentos electrónicos producidos y recibidos en el Ministerio de Defensa, y por tanto susceptibles de ser gestionados de acuerdo a las presentes directrices, incluyen, además de los expedientes y las agregaciones documentales, las siguientes tipologías, entre otras:

a) Correspondencia de entrada y salida.
b) Mensajes oficiales a través de sistemas de mensajería oficial.
c) Correos electrónicos.
d) Informes.
e) Transcripciones.
f) Contenidos digitales de formación o difusión, manuales técnicos y administrativos.

g) Registros de grabaciones de reuniones y conversaciones.
h) Instrucciones.
i) Fotografías, video e imágenes gráficas en soporte digital.
j) Transacciones de bases datos.
k) Páginas web (planificación, instantáneas y diseño).
l) Cartografía digital.
m) Datos de los sistemas de combate u otros sistemas que deban conservarse como evidencia.

No se consideran documentos electrónicos afectados por esta política los borradores, versiones no definitivas y notas o copias de trabajo.

1.2.2. Ciclo de vida de los documentos electrónicos

La PGDE-MINISDEF abarca todo el ciclo de vida de los documentos. Ello significa la aplicación de los procesos documentales normalizados desde el momento de su creación/captura y de manera continua durante las etapas activa, de vigencia administrativa y de conservación a largo plazo de la documentación.

1.3. DIRECTRICES DE LA PGDE-MINISDEF

La documentación del Ministerio de Defensa y la información contenida en la misma, serán tratadas como recurso de carácter estratégico. La gestión efectiva y eficiente de los documentos electrónicos constituye la base para la toma de decisiones a todos los niveles, la planificación de las misiones y operaciones, la gestión y servicios al personal tanto civil como militar, la respuesta a las interpelaciones parlamentarias y requerimientos judiciales, la continuidad digital y la preservación de la historia.

Los documentos, independientemente de su clasificación de seguridad, serán creados, almacenados, mantenidos, utilizados y conservados por medios electrónicos, salvo excepciones.

Los documentos permitirán documentar las acciones y actividades del Ministerio de Defensa tanto en tiempo de guerra como de paz; son evidencia de la estructura, organización, funciones, políticas, procedimientos, decisiones y actividades del Departamento y deben ser mantenidos de acuerdo a las directrices establecidas para el conjunto

de la Administración General del Estado y con las características específicas del ámbito de la defensa.

Los documentos electrónicos serán gestionados de acuerdo a las directrices establecidas en esta política y sus procedimientos e instrucciones derivadas.

Los requisitos de gestión de documentos electrónicos serán implementados en los sistemas de información y comunicaciones, donde se creen, capturen, controlen y conserven a lo largo del tiempo.

Los instrumentos necesarios para facilitar la gestión de los documentos electrónicos que deben desarrollarse y/o adaptarse y mantenerse adecuadamente para su aplicación normalizada en el Departamento son:

a) El cuadro de clasificación documental, que permite contextualizar y agrupar los documentos en relación con las funciones, procedimientos y actividades del Ministerio de Defensa.
b) El esquema de metadatos del Ministerio de Defensa e-EMMDEF, que establecerá las propiedades normalizadas que permitan la identificación, descripción, relación, interoperabilidad, trazabilidad del acceso, del uso y de las acciones realizadas sobre los documentos a lo largo de su ciclo de vida.
c) El calendario de conservación que, de acuerdo a lo establecido en el Reglamento de Archivos Militares (RAM), permitirá predefinir y automatizar los eventos de transferencia, expurgo o conservación a aplicar a lo largo del ciclo de vida de los documentos electrónicos.
d) Otros instrumentos como mapas documentales, vocabularios controlados, sistemas de codificación, etc. que se desarrollen de acuerdo a las necesidades específicas de la documentación.

Los documentos electrónicos cumplirán las condiciones necesarias para ser interoperables tanto internamente entre los componentes de los sistemas de información del Ministerio de Defensa, como con otros Organismos de la Administración Pública, siguiendo los requerimientos que establecen las Normas Técnicas de Interoperabilidad.

Los documentos electrónicos estarán protegidos según sus niveles de clasificación de acuerdo a lo establecido en la Política de Seguridad de la Información del Ministerio de Defensa y sus instrucciones deri-

vadas. No se deberán eliminar ni destruir documentos sin aplicar los protocolos de expurgo autorizados.

Los documentos esenciales serán identificados, protegidos y gestionados de manera que se asegure su disponibilidad en caso de catástrofe y puedan dar soporte a la continuidad de las actividades del Departamento.

Las copias auténticas de documentos electrónicos se generarán según el procedimiento instrumental descrito en el anexo 1 y estarán sujetas a esta política siempre que el análisis documental así lo determine.

Las copias de trabajo, los borradores y la documentación de apoyo informativo no serán objeto de esta política y serán destruidos cuando ya no se necesiten a decisión de las unidades productoras.

El personal del Ministerio de Defensa estará formado e informado de sus responsabilidades en relación con la gestión de documentos electrónicos y de la forma de proceder para cumplir con las mismas.

1.4. ÁMBITO DE APLICACIÓN

La PGDE-MINISDEF es de aplicación a la documentación electrónica del Ministerio de Defensa y cualquier norma interna que trate algún aspecto particular de la gestión de los documentos electrónicos del Departamento deberá estar alineada con esta política.

1.5. RIESGOS DERIVADOS DEL INCUMPLIMIENTO DE ESTA POLÍTICA

La gestión inadecuada de los documentos electrónicos puede originar riesgos para el Ministerio de Defensa en los siguientes aspectos[1]:

a) Operaciones presentes o futuras.
b) Toma de decisiones.

[1] Para el establecimiento de un plan de riesgos se puede tomar como referencia la UNE-ISO/TR 18128:2014. Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental. (http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053363) y el apartado «Risk management and contingency plans» del documento «Defence Records Management Policy Manual. Australian Government» (http://www.defence.gov.au/publications/manuals/polman3/polman3.pdf).

c) Pérdidas económicas.
d) Deterioro de la confianza pública.
e) Cumplimiento de sus obligaciones legales y defensa judicial.

El incumplimiento de esta política puede tener consecuencias para el Departamento, sus unidades y su personal, tanto civil como militar. La sospecha de incumplimiento en relación con el tratamiento o protección inadecuados, o la destrucción no autorizada de documentos electrónicos del Ministerio de Defensa, podrá ser investigada.

Una adecuada gestión documental implicará la elaboración de un Plan de Análisis de Riesgos que los identifique, controle, elimine y mitigue y prevea las consecuencias tanto para el Ministerio de Defensa como para los ciudadanos. Este Plan deberá estar en consonancia con las estrategias generales de gestión de riesgos de la Administración General del Estado y con el Plan Nacional de Emergencias y Gestión de Riesgos en el Patrimonio Cultural.

2. Marco de la PGDE-MINISDEF

2.1. ACTORES Y RESPONSABILIDADES

Los diferentes actores involucrados en la aplicación de la presente política, deberán tener asignadas las responsabilidades conforme a los niveles y funciones encomendadas. A tal fin, se establece el siguiente marco de responsabilidades:

a) Alta Dirección.
b) Nivel Corporativo.
c) Nivel Específico.

2.1.1. Alta Dirección

La Alta Dirección es responsable de la aprobación e impulso de la presente política y estará representada por:

a) El **Ministro de Defensa** que asume al más alto nivel, la aprobación e impulso de la PGDE-MINISDEF y ejerce las facultades que tiene conferidas en materia de clasificación de la información y determinación del régimen de acceso a los documentos electrónicos.

b) Los **responsables de los ámbitos específicos del Ministerio de Defensa** que son:
   1. Fuerzas Armadas, que se subdividen en:
      i. Estado Mayor de la Defensa
      ii. Ejército de Tierra
      iii. Armada
      iv. Ejército del Aire
   2. Secretaría de Estado de Defensa
   3. Subsecretaría de Defensa
   4. Secretaría General de Política de Defensa

A quienes corresponde:

1.º Asegurar en el ámbito de su competencia que sus responsabilidades en materia documental están definidas, asignadas y comunicadas.
2.º Impulsar, promover y difundir la política y coordinar la aplicación de la misma.
3.º Asegurar la disponibilidad de recursos para apoyar y mantener la política.
4.º Ejercer las facultades conferidas en materia de clasificación de la información y determinación del régimen de acceso a los documentos electrónicos.
5.º Impulsar las acciones de mejora que se precisen.

2.1.2. Nivel corporativo[2]

Este nivel funcional es responsable, en el ámbito del Departamento, en términos generales, de la dirección, coordinación, evaluación y supervisión de la aplicación de esta política. Estará integrado por:

a) La **Comisión Ministerial de Administración Digital del Ministerio de Defensa (CMAD)** es el órgano colegiado responsable del impulso y de la coordinación interna del Departamento y sus organismos públicos adscritos en materia de Administración Digital. También es responsable de mantener el enlace con

[2] Basado en la Política de Seguridad de la Información del Ministerio de Defensa (Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa).

los órganos y comisiones relacionadas con las tecnologías de la información y las comunicaciones del resto de la AGE. En materia de gestión documental le corresponde:

1.º Determinar el orden de prioridad en la planificación e implantación de la política de gestión de documentos electrónicos, de acuerdo con el plan de acción del Departamento para la transformación digital.
2.º Aprobar el Esquema de Metadatos del Ministerio de Defensa.
3.º Revisar los informes de supervisión y auditoria del cumplimiento de la política y adoptar y promover las mejoras y medidas correctoras.

b) El **órgano que ejerce la dirección del Sistema Archivístico de la Defensa**, que junto con los **Centros de Archivo** y la **Comisión Calificadora de Documentos de la Defensa**, es responsable de la aplicación de esta política en los aspectos funcionales y operativos de la gestión de documentos electrónicos y le corresponde:

1.º Planificar y fijar las necesidades para el desarrollo de los instrumentos metodológicos y requerimientos funcionales para la implantación de la política.
2.º Presentar y proponer el plan de aplicación de la PGDE-MINISDEF.
3.º Coordinar la designación de los interlocutores válidos para el apoyo, desarrollo e implementación de la gestión de documentos en el Ministerio y aportar especialistas en gestión de documentos.
4.º Definir y trasladar los requerimientos funcionales de la política según el análisis documental realizado.
5.º Planificar y ejecutar el plan y el programa de formación en materia de gestión de documentos electrónicos, en el marco del plan de transformación digital del Departamento.
6.º Impulsar la formación del personal especializado en la gestión de documentación electrónica para el desarrollo de habilidades y competencias en sus áreas de responsabilidad.
7.º Proporcionar soporte y apoyo, a través de sus centros de archivo, a las acciones de formación, difusión e implanta-

ción de la gestión de los documentos electrónicos, en los ámbitos y unidades del Departamento.

8.º Documentar y gestionar electrónicamente la documentación normativa y funcional derivada de esta política, facilitando su acceso al órgano que ejerce la dirección de los sistemas y tecnologías de información y comunicaciones del Ministerio de Defensa.

9.º Desarrollar los procedimientos de las operaciones en los procesos de gestión documental y apoyar en la implementación de los mismos.

10.º Definir, aprobar y mantener actualizados el Cuadro de Clasificación y el e-EMMDEF en función de las necesidades identificadas.

11.º Estudiar y elaborar las propuestas de valoración sobre plazos de conservación, transferencias y/o eliminación de los documentos electrónicos. Coordinar las propuestas de los distintos ámbitos del Departamento en lo que afecta a los documentos esenciales.

12.º Velar por la correcta aplicación de los derechos de acceso sobre los documentos cuya custodia esté transferida al correspondiente centro de archivo.

13.º Resolver los conflictos y propuestas en materia de solicitudes de acceso a través de la Comisión Calificadora de Documentos de la Defensa.

14.º Elevar a la Comisión Ministerial de Administración Digital del Departamento los informes derivados de la supervisión y auditoria del cumplimiento de la PGDE-MINISDEF.

c) El **órgano que ejerce la dirección de los sistemas y tecnologías de la información y las comunicaciones del Ministerio de Defensa**, que será responsable de:

1.º Incluir el programa y las necesidades de la gestión de documentos electrónicos dentro de la estrategia de tecnologías de la información y comunicaciones, fijando las necesidades detectadas y elaborando un plan de acción para la transformación digital.

2.º Aportar los recursos humanos necesarios y designar los especialistas interlocutores válidos para el desarrollo e implementación de la gestión documental.
3.º Planificar y ejecutar la formación en las aplicaciones de gestión de documentos electrónicos, en coordinación con los responsables del SAD.
4.º Documentar técnicamente los sistemas y las aplicaciones de gestión de documentos, e incorporar dicha documentación al entorno de gestión electrónica de documentos, proporcionando acceso a los responsables del SAD designados, de forma que se coordinen las actuaciones funcionales y tecnológicas.
5.º Diseñar, configurar, mantener e implementar el programa de gestión de documentos electrónicos en los sistemas y tecnologías del Departamento.
6.º Llevar el registro de metadatos y detectar las necesidades de actualización del e-EMMDEF en coordinación con la los responsables del SAD.
7.º Implementar el Cuadro de Clasificación en las aplicaciones de gestión de documentos.
8.º Determinar los documentos esenciales en colaboración con los distintos ámbitos del Departamento y aplicar las medidas de protección adecuadas a los mismos.
9.º Implementar los procesos de gestión documental sobre las aplicaciones.
10.º Determinar la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa a los entornos en que se gestionan los documentos electrónicos de acuerdo con su clasificación y régimen de acceso a lo largo de su ciclo de vida.
11.º Aplicar las medidas pertinentes en relación con los documentos electrónicos desclasificados y proceder a su transferencia al entorno de archivo electrónico cuando deban ser objeto de conservación a largo plazo.
12.º Implementar los controles en los sistemas y aplicaciones de gestión de documentos para preservarlos en las condiciones adecuadas y garantizar su integridad, autenticidad y disponibilidad durante todo su ciclo de vida.

13.º Implementar y recopilar la traza de las acciones realizadas sobre los documentos, manteniéndola por el tiempo que se determine en función de los requerimientos establecidos en la Política de Seguridad de la Información Ministerio de Defensa.
14.º Proporcionar los datos que se originen en los sistemas, a través de las explotaciones necesarias, que posibiliten la supervisión y auditoría de las acciones de aplicación de esta política.

2.1.3. Nivel específico

En este nivel los responsables en la aplicación de la PGDE-MINISDEF serán:

a) Ámbitos y unidades[3] que deberán:

1.º Desarrollar y evaluar en su ámbito la aplicación de la gestión de los documentos electrónicos.
2.º Garantizar que el personal a su cargo conozca esta política y que esté plenamente capacitado para aplicarla.
3.º Designar los interlocutores para el desarrollo e implementación de la gestión de documentos dentro de su ámbito de competencia.
4.º Ejecutar los procesos de creación y captura de documentos electrónicos recogidos en el apartado 4 de esta política de acuerdo a las reglas establecidas.
5.º Ejecutar los procesos de clasificación documental y descripción recogidos en el apartado 5 de esta política de acuerdo a las reglas establecidas.
6.º Proponer la aplicación del régimen de acceso y utilización de los documentos y series documentales para cumplir con lo estipulado en la legislación sobre derechos de acceso.
7.º Aplicar las mejoras y medidas adoptadas como resultado de la supervisión y auditoría realizada en cumplimiento de la PGDE-MINISDEF.

Los **Ámbitos** además deberán:

1.º Trasladar las necesidades y proponer altas, bajas o modificaciones del Cuadro de Clasificación de acuerdo a las funciones y actividades en el ámbito de su competencia.

[3] Ámbitos específicos del Departamento y sus unidades dependientes.

2.º Determinar sus documentos esenciales en colaboración con el órgano que ejerce la dirección de los sistemas y tecnologías de la información y las comunicaciones del Ministerio de Defensa.

Las **Unidades** además deberán:

1.º Definir cómo aplicar los procesos de gestión documental a sus documentos.
2.º Controlar, evaluar y supervisar la correcta aplicación de la gestión de los documentos electrónicos y trasladar las incidencias a los responsables corporativos.

b) Custodios, elaboradores y usuarios: definidos en la Instrucción 64/2015, de 7 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas de seguridad de la información para la elaboración, clasificación, cesión, distribución y destrucción de la información del Ministerio de Defensa.

Los **custodios** son las personas u organismos responsables de guardar y proteger los documentos desde su elaboración. En el entorno electrónico asumirán la responsabilidad de:

1.º Validar en sus respectivas unidades la adecuada aplicación de los procedimientos de captura, clasificación y descripción de los documentos que se describen en los apartados 4 a 6 de este documento.
2.º Proponer la aplicación del régimen de acceso y utilización de los documentos y series documentales para cumplir con lo estipulado en la legislación en materia de derechos de acceso.
3.º Velar por la correcta aplicación de los derechos de acceso y la seguridad a los documentos cuya custodia tenga encomendada.

Los **elaboradores**, son las personas u organismos que materializan una información electrónica en forma de documento. Serán responsables de:

1.º Ejecutar los procesos de creación y captura de documentos electrónicos recogidos en el apartado 4 de esta política de acuerdo a las reglas establecidas.

2.º Ejecutar los procesos de clasificación documental y descripción recogidos en el apartado 5 de esta política de acuerdo a las reglas establecidas.
3.º Determinar el régimen de uso oficial o uso público de la documentación electrónica no clasificada, de acuerdo con la legalidad vigente.

Los **usuarios** son las personas a las que el custodio de los documentos permite el acceso a los mismos. Deberán utilizar los documentos ateniéndose a las normas de seguridad del Departamento y a la normativa vigente en materia de difusión y publicación de documentos de carácter público.

2.2. PLANIFICACIÓN

Para llevar a cabo la presente política y velar por su coherencia con los objetivos estratégicos del Ministerio de Defensa, esta se debe coordinar con los planes de suministro de recursos materiales de los sistemas de información y comunicaciones y con los recursos de personal necesario para asumir las nuevas responsabilidades.

El desarrollo de la PGDE-MINISDEF requerirá la elaboración y ejecución de un plan de implantación que establecerá:

a) Los objetivos y líneas de actuación.
b) Las acciones concretas a desarrollar en todas las unidades del Ministerio de Defensa.
c) El programa de tratamiento de los documentos.
d) Las operaciones de los procesos de gestión de los documentos electrónicos en las unidades del Departamento.
e) La determinación de los recursos humanos, técnicos y materiales necesarios para la ejecución del plan.
f) La planificación temporal del proyecto.

Este plan formará parte del Plan de Transformación Digital del Ministerio de Defensa y deberá estar vinculado a las etapas e hitos marcados para la transformación de los procesos de gestión internos en electrónicos y al desarrollo del puesto de trabajo digital.

Además, estará supeditado a lo que establezca el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones en

relación a las infraestructuras, servicios y aplicaciones necesarias para implementar el programa de tratamiento de los documentos electrónicos.

2.3. DESARROLLO NORMATIVO Y DOCUMENTACIÓN

Las directrices en materia de gestión de documentos electrónicos del Ministerio de Defensa se concretarán en un desarrollo normativo que se realizará en tres niveles:

a) En el primer nivel: se encuentra la presente política de gestión de documentos electrónicos respaldada al más alto nivel y aprobada mediante el desarrollo normativo más adecuado o que corresponda.
b) En el segundo nivel: las normas que desarrollan a la anterior:
    1.º Los instrumentos de gestión documental de uso normalizado en el Ministerio de Defensa.
    2.º Las directrices específicas para la aplicación de los procesos documentales, en determinados ámbitos de actividad: operaciones, personal, atención sanitaria, justicia militar, etc.
    3.º Las directrices específicas para la aplicación de los procesos documentales a determinadas tipologías de documentos: mensajes electrónicos, páginas web, imagen digital, grabaciones sonoras en soporte digital, registros en bases de datos, etc.
    4.º Las directrices específicas para la aplicación de los procesos documentales en los diferentes niveles de intensidad en los que se puedan desarrollar las operaciones.
    5.º Y todas aquellas que se estimen necesarias.
c) En el tercer nivel: instrucciones, guías y procedimientos que concretan aspectos prácticos de la gestión documental y todas aquellas que se estimen necesarias.

Se tendrán en cuenta las directrices que establezcan las autoridades en materia de administración digital y las autoridades calificadoras y archivísticas competentes, de acuerdo con la legislación.

Además de los documentos de carácter normativo, se llevará registro y archivo en soporte electrónico de toda la documentación derivada o relacionada con la aplicación de esta política que sea evidencia del cumplimiento de la misma a efectos de supervisión y auditoría.

2.4. ACTUALIZACIÓN DE LA POLÍTICA

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá a la Unidad responsable de esta política, que es el órgano que ejerce la dirección del Sistema Archivístico de la Defensa que realizará el seguimiento de la implantación de la misma y propondrá las revisiones necesarias a la CMAD.

Las revisiones de los anexos de la PGDE-MINISDEF no requerirán publicación formal.

El cuerpo deberá ser revisado con una periodicidad mínima de dos años y publicada una nueva norma cuando los cambios lo requieran.

2.5. FORMACIÓN, DIFUSIÓN Y APOYO

La formación y difusión en materia de gestión de documentos electrónicos se adecuará a la estrategia de gestión del cambio y de desarrollo de capacidades digitales para el personal del Ministerio de Defensa en el marco del Plan de Transformación Digital.

Todo el personal del Departamento deberá recibir asistencia y formación para desarrollar las habilidades y competencias necesarias respecto a la gestión de los documentos electrónicos en el ámbito de su responsabilidad.

El órgano que ejerce la dirección del Sistema Archivístico de la Defensa, que es responsable de la aplicación de esta política en los aspectos funcionales y operativos de la gestión de documentos, elaborará un plan de formación para que todo el personal del Ministerio de Defensa, que deba operar con los documentos electrónicos, pueda aplicar correctamente las directrices de esta política y las normas que de ella emanen. Dicho plan estará alineado con los que desarrolle el Órgano que ejerce la dirección de los sistemas y tecnologías de información y comunicaciones del Ministerio de Defensa en el marco de los objetivos de transformación digital. En los casos en que se considere más eficiente, las acciones de formación se realizarán en coordinación con los responsables de las aplicaciones tecnológicas.

En las acciones de formación se emplearán todos aquellos medios presenciales o virtuales que faciliten el cumplimiento de los objetivos de aprendizaje propuestos.

El programa de formación comprenderá tres categorías de acciones:

a) Formación en la concienciación de la aplicación de esta política:

   1.º Se elaborará y pondrá a disposición de todo el personal en la plataforma del campus virtual del Ministerio de Defensa un curso introductorio de corta duración sobre la aplicación de la PGDE-MINISDEF. Se recomendará que todo el personal que trabaja en el Departamento, y recibe o produce documentos en el desempeño de su actividad profesional, complete este curso básico. Igualmente se deberá incluir en la formación del personal de nueva incorporación.
   2.º En coordinación con las unidades responsables, se revisarán los programas de formación del Ministerio de Defensa en los que se deban incorporar módulos específicos o consideraciones concretas respecto a la gestión electrónica de documentos.

b) Formación del personal especializado en gestión de documentos electrónicos:

   1.º Se determinarán qué capacidades se deben actualizar para el personal que desempeña funciones técnicas en el marco del SAD y que deba asumir nuevas responsabilidades en el marco de la presente PGDE-MINISDEF.
   2.º A través de programas de formación reglados, cursos especializados, o tutorías específicas, se pondrán los medios necesarios para asegurar que estas personas están capacitadas con formación y experiencia adecuadas para su desempeño. Se llevarán a cabo revisiones periódicas de la capacitación de este personal.

c) Formación en la aplicación de los procesos de gestión de documentos electrónicos:

   1.º Se publicará y distribuirá electrónicamente el Manual de Archivos de Oficina, una vez incorporados los aspectos que afectan a la gestión de los documentos electrónicos.
   2.º Se elaborarán programas de formación específicos adaptados tanto a los hitos de implantación como a su aplicación en distintos entornos y a distintas tipologías de documentos.

Dichos programas deberán cursarse por los gestores de las unidades implicados en cada proceso de gestión documental y en la toma de decisiones en relación con la documentación bajo su responsabilidad.

3.º Se elaborarán programas específicos para los responsables de la gestión de los documentos electrónicos en las unidades del Ministerio de Defensa.

Anualmente se incluirán en el programa de formación del Ministerio de Defensa actuaciones destinadas a la formación continua y capacitación del personal responsable de la ejecución y del control de la gestión de los documentos electrónicos y de su tratamiento y conservación en repositorios o archivos electrónicos.

La unidad responsable de la aplicación de esta política planificará y llevará a cabo las acciones necesarias para comunicar y difundir la política y la documentación normativa que emane de la misma, incidiendo en aspectos como la responsabilidad de la gestión de los documentos electrónicos, evitar riesgos, capturar y mantener el conocimiento de la organización, o preservar el patrimonio documental. Se podrán realizar presentaciones, folletos divulgativos, publicaciones en la intranet del Ministerio de Defensa y todos aquellos medios que faciliten su conocimiento en todos los niveles del Departamento.

La unidad responsable de la aplicación de esta política prestará apoyo –en la medida de sus recursos– a las Unidades del Ministerio de Defensa que lo soliciten:

a) En la realización del análisis documental asociado a la transformación digital de los procedimientos y procesos de trabajo.
b) En la aplicación práctica de los procesos documentales que se desarrollan en esta política.
c) En la resolución de dudas e incidencias que surjan en el periodo de implantación.

2.6. SUPERVISIÓN Y AUDITORÍA

La supervisión de la aplicación de esta política, responsabilidad colegiada entre el órgano que ejerce la dirección de los sistemas y tecnologías de la información y comunicaciones y el órgano que ejerce

la dirección del Sistema Archivístico de la Defensa, se llevará a cabo mediante las siguientes acciones:

a) Revisiones de las actividades de tratamiento de los documentos electrónicos realizadas a nivel de Departamento o unidad organizativa.
b) Evaluación de los niveles de ejecución del plan de implantación de la política, del programa de tratamiento de los documentos así como de los resultados obtenidos.
c) Supervisión de la correcta aplicación de los controles establecidos en los procedimientos de gestión de documentos electrónicos.

Con una periodicidad mínima de 5 años se llevarán a cabo procesos de auditoría interna para evaluar la eficacia de la gestión de los documentos electrónicos y el grado de cumplimiento de la normativa, con el objeto de proponer acciones de mejora o correctivas.

La supervisión se realizará al menos en los siguientes momentos:

a) Una vez al año.
b) En los hitos planificados de implantación.
c) De manera ocasional, cuando se detecte un riesgo en el proceso de gestión documental.

La gestión de los documentos electrónicos del Departamento, podrá estar sujeta a procesos de supervisión o auditoría externa. Para evaluar el cumplimiento del ENI en lo que afecta a la gestión de los documentos electrónicos, se recabarán los datos del cuestionario de la Guía de adecuación al Esquema Nacional de Interoperabilidad que se recoge en el anexo 2.

2.7. OPERACIÓN DE LA GESTIÓN DOCUMENTAL Y PROGRAMA DE TRATAMIENTO DE LOS DOCUMENTOS

La operación de la gestión documental consistirá en la ejecución de los procesos de gestión documental[4] en los entornos, las aplicaciones y los sistemas de información que posibilitan el tratamiento de los documentos electrónicos por medios digitales.

[4] Los procesos de gestión documental son: la creación y captura, la clasificación y la descripción y la calificación, conservación, transferencia y eliminación que serán definidos en los apartados 4, 5 y 6 de esta política.

Para ello, se deberá desarrollar un programa de tratamiento de los documentos que contemple, al menos, los siguientes aspectos técnicos:

a) Identificación de los requerimientos funcionales para el tratamiento de los documentos electrónicos y su inserción o vinculación con las tecnologías y sistemas de información y comunicaciones empleados en el Ministerio de Defensa. Estos requerimientos estarán basados en los establecidos por las Normas Técnicas de Interoperabilidad y los estándares de referencia en el ámbito de los organismos internacionales de seguridad y defensa.
b) Especificación de las operaciones de los procesos documentales y de las aplicaciones o tecnologías más adecuadas. Estas deben de atenerse a las directrices de la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa y su desarrollo y planificación en cuanto a servicios e infraestructuras, seguridad, normalización técnica, recursos, gestión de la información y el conocimiento y comunicación.
c) Identificación de los riesgos inherentes al tratamiento de los documentos electrónicos en las aplicaciones y los medios para su mitigación.
d) Planificación de desarrollo e implementación de los procesos y controles de gestión de los documentos, en las aplicaciones o sistemas que se hayan determinado.
e) Establecimiento de los mecanismos de supervisión periódica del funcionamiento de las aplicaciones de acuerdo con las necesidades del Ministerio de Defensa y los objetivos establecidos.
f) Establecimiento de los mecanismos de gestión, mantenimiento y actualización y planes de contingencia de los entornos, sistemas y aplicaciones en que se gestionan los documentos.

Las decisiones tecnológicas relativas a la implantación, prevista en el art. 17.1 de la LPAC, *del archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados,* deberán adoptarse para que sea efectivo su cumplimiento entre octubre de 2017 y octubre de 2018, que es el plazo máximo establecido en la Disposición Transitoria Segunda de la ley.

A falta de clarificación adicional de este concepto, el archivo único electrónico puede aplicarse desde un punto de vista organizativo (prácticas y procesos y servicios comunes de gestión de documentos que no impliquen un único lugar de almacenamiento) o técnico, optando por un repositorio único. La decisión debe estar basada en los requisitos operativos de la situación, en las necesidades y características de los sistemas de información del Ministerio de Defensa relacionados con la producción o almacenamiento de documentos: se puede optar por la fórmula mixta de repositorio único finalista –de procedimientos finalizados transferidos a situación de archivo definitivo (SGDEA)– y la combinación de distintas soluciones que coexistan en la situación de archivo activo cumpliendo unos requerimientos comunes en relación con la gestión documental.

Por la complejidad propia de los Sistemas de Información del Ministerio de Defensa, en una solución mixta se deberán tener en cuenta los siguientes criterios:

a) El diseño, desarrollo y mejora de los sistemas de información debe incorporar las consideraciones necesarias respecto a la gestión y preservación de los documentos electrónicos según lo establecido en sus calendarios de conservación.
b) En los nuevos sistemas en que se crean o reciben documentos, estos podrían ser gestionados electrónicamente implementando los requisitos de gestión de documentos dentro de las propias aplicaciones o transfiriendo los documentos a repositorios específicos de soluciones de gestión documental que cumplan con los requerimientos establecidos.
c) Para los sistemas ya existentes se deberá valorar la necesidad y oportunidad de aplicar los requerimientos en las propias aplicaciones y/o transferir los documentos a una solución de gestión documental y repositorio electrónico que cumpla con dichos requerimientos asegurando la disponibilidad de la información contenida en los mismos.

Se minimizará, en la medida de lo posible, el impacto sobre la operatividad de los sistemas, sobre el usuario y sobre la unidad a la que apoyan.

Los responsables del órgano que ejerce la dirección de los sistemas y tecnologías de información y comunicaciones del Ministerio de Defensa estudiarán –para aquellos procedimientos administrativos que no contengan documentación clasificada– la adhesión voluntaria a la/s plataformas y servicios de archivo electrónico que establezca al efecto la AGE[5].

La solución tecnológica que se implante en el Ministerio de Defensa deberá garantizar que los documentos electrónicos se almacenen en un formato que permita garantizar su autenticidad, integridad y conservación a largo plazo, así como su consulta, con independencia del tiempo transcurrido desde su emisión.

Los documentos y expedientes electrónicos deberán cumplir los requerimientos técnicos para ser interoperables:

a) Entre componentes de los sistemas de información y comunicaciones del propio Ministerio de Defensa.
b) Con organismos de la Administración Pública de España.
c) Con las organizaciones y estructuras operativas internacionales.

[5] La no adhesión deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

3. Esquema de metadatos y su aplicación a los procesos de gestión de los documentos electrónicos

3.1. CONCEPTO Y PROPÓSITO DE LOS METADATOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

Los metadatos se definen como «datos sobre los datos». En el contexto de la gestión de los documentos electrónicos, los metadatos son los datos que describen el contexto, contenido y estructura de los documentos, así como su gestión a lo largo del tiempo.

Los metadatos son información estructurada que puede usarse para identificar, autenticar y contextualizar los propios documentos y expedientes, los actores, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan, así como las políticas que los rigen.

Los metadatos deben aportar la información necesaria para la comprensión de los documentos electrónicos, de las relaciones existentes entre ellos y de las transacciones que los crearon y utilizaron. Asimismo, deben permitir identificar un documento en el contexto de las funciones y actividades a que corresponde y posibilitar la recuperación de los documentos, su conservación y gestión a lo largo del tiempo.

Para el uso de los metadatos de la gestión de los documentos electrónicos será necesario que el Departamento elabore una normativa de gestión de datos de Defensa[6] para poder:

a) Facilitar el intercambio de datos y la interoperabilidad entre los sistemas de información.
b) Mejorar la eficiencia en el desarrollo y mantenimiento de los sistemas de información.

Adicionalmente se conseguiría:

a) Facilitar la estandarización de las descripciones de los documentos atendiendo a sus diferentes tipologías.
b) Facilitar la implementación de sistemas y aplicaciones específicas para gestionar los documentos electrónicos.
c) Mejorar la recuperación y difusión de la información, siempre de acuerdo a las condiciones de acceso y seguridad establecidas.
d) Asegurar la preservación de la documentación a lo largo del tiempo sin pérdida de sus características de autenticidad, integridad y disponibilidad.
e) Demostrar conformidad con las NTI y estándares de metadatos para la gestión de documentos de uso internacional.

3.2. ESQUEMA DE METADATOS DEL MINISTERIO DE DEFENSA

Los responsables de la gestión de los documentos, en coordinación con los futuros responsables de gestión de datos del Ministerio de Defensa, elaborarán el e-EMMDEF.

El esquema establecerá el conjunto de metadatos autorizados para la gestión de los documentos en el Ministerio de Defensa y las reglas para su uso y gestión, específicamente las relacionadas con la semántica, la sintaxis y la obligatoriedad de los valores.

El e-EMMDEF se basará en el Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), disponible en el Centro de Interoperabilidad Semántica y en los esquemas y perfiles

[6] Hubo un primer desarrollo normativo en 2005 que se encuentra actualmente obsoleto por lo que se ve necesario actualizarlo y revisarlo.

de aplicación elaborados por otros organismos internacionales de la Seguridad y la Defensa, así como los específicos de las distintas tipologías documentales empleadas en el ámbito de la defensa.

El e-EMMDEF se incluirá en un Registro de Metadatos de Defensa[7] que constituirá el vehículo de estandarización de los datos utilizados en el Departamento.

3.3. ENFOQUE DE IMPLEMENTACIÓN DE LOS METADATOS

Las Normas Técnicas de Interoperabilidad establecen que 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.

El e-EMMDEF se definirá para que los metadatos se implementen en los sistemas de información bajo un modelo de multientidad, tal como recomiendan las buenas prácticas al respecto y se expone en el anexo 3 de esta política. Ello significa emplear las cinco entidades previstas, tanto en los estándares internacionales, como en el e-EMGDE: documento, agente, actividad, regulación y relación[8]. Esto permite crear los metadatos de una entidad una vez (ejemplo: un agente) y reutilizarlos tantas veces como se necesite para relacionarlo con los documentos, o las regulaciones que produce o las funciones y actividades que desempeña en relación con los documentos.

En los entornos de gestión de documentos, estos no se crean por azar, sino porque existen determinados vínculos con otras entidades: así, un documento es creado, controlado, versionado, etc., por un agente, y un agente lo crea, controla, versiona, etc., en el ejercicio

[7] Se deberá establecer un registro único y corporativo de metadatos en el Ministerio de Defensa. Este Registro deberá constituir el vehículo de estandarización de los elementos de datos utilizados en el Departamento. Mediante un proceso continuo de acuerdo y registro, se conseguirán definiciones de datos únicas y estandarizadas que deberán ser usadas en los sistemas de información que las requieran.

[8] Documento: documento simple/expediente/agregación/serie/fondo/grupo de fondos. Agente: persona/dispositivo/órgano o institución. Actividad: acción/función/función marco. Relación: entre documento, agente y actividad. Regulación: normativa que relaciona documento, agente y actividad.

de una función. La función permite u obliga al agente a crear el documento, en el ejercicio de competencias dadas por la regulación; el agente es obligado a, o se le permite, crearlo, porque ejerce una función regulada; y el documento da evidencia de la actividad y de que esta es conforme con la regulación.

La adopción de este enfoque, aunque presenta mayor dificultad técnica, es más flexible para aplicarse a entornos de gestión de documentos de naturaleza compleja como es el caso del Ministerio de Defensa. En el anexo 3 se incluyen las recomendaciones y documentos de referencia para facilitar su implementación.

Los aspectos técnicos de implementación de los metadatos para la gestión de documentos electrónicos, se definirán en el diseño del programa de gestión de documentos electrónicos valorando las diferentes posibilidades técnicas de almacenamiento de los metadatos tales como el encapsulado, la incrustación de los metadatos en los propios documentos o el almacenamiento en repositorios vinculados a los objetos que describen.

La revisión periódica, mantenimiento y actualización del e-EMMDEF será responsabilidad del órgano que ejerce la dirección del SAD de acuerdo con los futuros responsables de gestión de datos del órgano que ejerce la dirección de los sistemas y tecnologías de información y comunicaciones del Ministerio de Defensa.

3.4. APLICACIÓN DE LOS METADATOS EN LA OPERACIÓN DE LOS PROCESOS DOCUMENTALES

Los metadatos apoyan los procesos de gestión de documentos electrónicos:

a) Protegiendo el uso de los objetos de información como prueba y asegurando su accesibilidad y disponibilidad a lo largo del tiempo.
b) Facilitando la comprensión de los objetos de información.
c) Contribuyendo a garantizar la autenticidad, fiabilidad e integridad de los objetos de información.
d) Respaldando la gestión del acceso, la privacidad y los derechos de propiedad intelectual.
e) Sirviendo de base para una recuperación eficiente.

f) Respaldando las estrategias de interoperabilidad, permitiendo que se incorporen oficialmente al sistema objetos de información creados en diversos entornos administrativos y técnicos y que se mantengan durante el tiempo que sea necesario.
g) Proporcionando vínculos lógicos entre los objetos de información y su contexto de creación y gestión, manteniéndolos de forma estructurada, fiable e inteligible.
h) Facilitando la identificación del entorno tecnológico en que los objetos de información fueron creados o se incorporaron al sistema y la gestión del entorno tecnológico en el que se han mantenido, de modo que puedan ser reproducidos como documentos auténticos cuando se necesiten.
i) Facilitando la migración eficiente y exitosa de objetos de información de un entorno o plataforma informáticos a otro, o cualquier otra posible estrategia de conservación.

Los metadatos deben definir los documentos y sus agrupaciones en los procesos de captura, clasificación y descripción fijándolos en su contexto y estableciendo los controles necesarios para su gestión. Los documentos pueden disponer de metadatos adicionales previos referentes a su creación, recepción (vía registro u otro medio de intercambio) o al proceso de digitalización en origen. A lo largo del tiempo, los metadatos continuarán acumulando información relacionada con el contexto del uso y acceso de los documentos electrónicos mediante traza de auditoría, así como de las acciones de transferencia, eliminación o conservación que se realicen sobre los documentos. Los metadatos aplicados a los objetos de información durante su vida activa o de gestión van a seguir utilizándose durante todo su ciclo de vida para facilitar las búsquedas e investigaciones futuras.

En la configuración de los objetos que representan los niveles de agrupación de los documentos –ver apartado 5– se podrán incorporar metadatos que se hereden del nivel superior a los inferiores: desde la serie al expediente y desde el expediente o agregación documental al documento propiamente dicho.

Hay que evitar siempre que sea posible la asignación manual, siendo responsabilidad de las aplicaciones y sistemas transaccionales informar al/los repositorios documentales de los metadatos que requieren los documentos.

Se debe 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 del Ministerio de Defensa a lo largo del tiempo manteniendo permanentemente su relación con los documentos u objetos de información descritos.

Hasta completar el desarrollo y aprobación definitiva del e-EMMDEF, la presente política incluye en el anexo 3 la relación de los metadatos obligatorios y complementarios:

a) Requeridos en las Normas Técnicas de Interoperabilidad de Documento Electrónico y Expediente Electrónico.
b) Adoptados a partir del e-EMGDE en las políticas de otros departamentos de la AGE.

Además en los siguientes apartados, se incluyen los metadatos mínimos aplicables a cada uno de los procesos de gestión documental.

4. Procesos de creación y captura de documentos electrónicos

4.1. IDENTIFICACIÓN Y ANÁLISIS DOCUMENTAL

El diseño de los procesos de gestión de documentos electrónicos del Ministerio de Defensa deberá realizarse a partir de la identificación y el análisis documental de los procesos de trabajo desarrollados en el desempeño de las funciones que el Ministerio tiene encomendadas.

Dicho análisis deberá determinar los requisitos para la creación, captura y control de los documentos que se crean, reciben y utilizan, en relación con las operaciones que desarrollan y definir los vínculos contextuales entre los mismos para contribuir a su ordenación y agrupación lógica. Comprenderá la recopilación de información sobre:

a) El contexto regulatorio de los documentos del Ministerio de Defensa, en especial cuándo pueden aplicar requerimientos específicos para la documentación establecidos por la normativa propia o por los organismos internacionales de seguridad y defensa.
b) Las funciones, actividades y procedimientos que dan origen a los documentos, base para el desarrollo del cuadro de clasifica-

ción documental del Departamento que se refiere en el apartado 5 de esta política.

c) Los procesos de trabajo, con el objeto de identificar los documentos resultantes de los mismos y sus características: los vínculos con otros procesos; los eventos que deben crear documentos y abrir expedientes; los momentos de creación y captura; los metadatos complementarios que se requiriesen para los procesos de gestión documental, los requerimientos de firma, los responsables de los mismos, la clasificación de seguridad aplicable, los entornos de sistemas de información con que se relacionan, los sistemas de codificación aplicados, etc.
d) La identificación de los documentos esenciales de cara a la calificación que se establece en el apartado 6 de esta política.

Se procederá a su validación por parte de los responsables e involucrados en los procesos de trabajo para garantizar que los datos recopilados están completos de cara a su implementación en los sistemas de información.

El desarrollo de la metodología de identificación y análisis documental, estará alineado con la determinación de los requisitos y directrices de seguridad de la información que afecten a la documentación del Departamento, establecidos en las Normas de Seguridad de la Información en los documentos (SEGINFODOC) y otra normativa de desarrollo.

Será aplicable a todas las unidades cuando:

a) Se aborde el análisis de los procesos y procedimientos de trabajo de cara a su transformación digital.
b) Con carácter previo a cualquier implementación en los sistemas de información que deba aplicar los procesos de gestión documental que se establecen en esta política y sus instrucciones derivadas.
c) Cuando la documentación ya existente deba ser transferida al archivo electrónico único para su conservación a lo largo de su ciclo de vida.
d) Con carácter previo a abordar trabajos de digitalización de fondos documentales en soporte papel para su incorporación a los sistemas en que se gestionan los documentos electrónicos.

4.2. CREACIÓN DE DOCUMENTOS

La creación de documentos deberá realizarse preferiblemente en el momento más próximo a la actividad, y por las personas que tengan asignada la competencia o función.

Los documentos podrán tener origen:

a) Externo: recibidos del ciudadano, otras administraciones u organismos nacionales e internacionales.
b) Interno: producidos por cualquiera de las unidades o personal civil y militar del Ministerio de Defensa en el ejercicio de sus funciones y desempeño de su actividad.
c) Colaborativo: producidos e intercambiados en condiciones de colaboración con instituciones o entidades nacionales e internacionales relacionadas con las actividades y funciones del Ministerio de Defensa.

Las características del documento, ya sea de origen externo, interno o colaborativo, se mantendrán inalterables en los casos en que terceras partes (empresas o personas) tramiten, gestionen o actúen en nombre del Ministerio de Defensa en virtud de contratos o convenios.

Los requisitos específicos que deban aplicarse en la creación o recepción de los documentos electrónicos (por ejemplo: uso de plantillas o formularios normalizados, sistemas específicos de codificación, control de versiones, formatos electrónicos específicos, etc.) serán identificados en el análisis documental.

Los documentos se crearán con firma electrónica cuando sea requerida según establece la LPAC o se determine por la regulación y procedimientos específicos del Ministerio de Defensa. Dicha ley contempla como excepción, en todo caso, y siempre debiéndose identificar el origen de estos documentos, que no requerirán firma electrónica los documentos electrónicos emitidos que se publiquen con carácter meramente informativo, así como aquellos que no formen parte de un expediente administrativo.

El tipo de firma y el servicio a emplear para la misma se atendrá a lo que establezca el órgano que ejerce la dirección de los sistemas y tecnologías de información y comunicaciones del Departamento en materia de firma electrónica.

La creación de documentos en el Ministerio de Defensa podrá producirse en distintos escenarios: entornos ofimáticos, entornos de colaboración, aplicaciones específicas de gestión o tramitación, sistemas de gestión de proyectos, dispositivos electrónicos, registros de entrada, sistemas de intercambio de información, etc. En función de las características de cada situación se deberá establecer el estado, momento y los mecanismos mediante los que se procederá a la captura de los documentos según los requerimientos.

4.3. CAPTURA DE DOCUMENTOS

La captura de documentos electrónicos se produce en el momento en que estos se incorporan en el sistema de gestión documental, cumpliendo los requerimientos de esta política. En ese punto se establece la relación fundamental que permanecerá inalterable entre el documento y su creador/receptor y el contexto en que se creó/recibió por medio de los correspondientes metadatos.

La creación y captura de los documentos no necesariamente tienen que coincidir en el tiempo; como buena práctica se recomienda, siempre que sea posible, que la captura se realice en el momento más cercano a la recepción del documento o a su producción en un estado definitivo.

Las decisiones sobre qué documentos serán capturados y cuáles no, en cada uno de los procesos, se basarán en la identificación y análisis documental llevado a cabo. Teniendo esto en cuenta, no deberán capturarse borradores, versiones de documentos ni documentos efímeros, salvo que circunstancias excepcionales así lo requieran.

El momento de la captura y los métodos de integración de esta en los procesos de trabajo y en las aplicaciones, se definirán desde el punto de vista técnico en el diseño del programa de gestión documental y se aplicará en cada caso en base al análisis documental. En dicho análisis se determinará asimismo el tipo de agrupación de los documentos: series, expedientes u otro tipo de agregaciones documentales, que sea necesario crear como paso previo a la captura de los documentos electrónicos.

El proceso de captura en los sistemas de información deberá aportar las condiciones para garantizar la autenticidad, fiabilidad, integridad y disponibilidad de los documentos mediante:

a) La asignación de metadatos de identificación y de contexto obligatorios definidos en el e-EMGDE. Hasta el desarrollo del e-EMMDEF se adoptarán inicialmente los metadatos mínimos obligatorios de captura exigidos para el intercambio por las NTI de documento electrónico y de expediente electrónico.
b) La identificación unívoca de los documentos y los expedientes electrónicos y de su contexto a través de identificadores únicos que sean adaptables al formato exigido por las NTI de documento y expediente electrónico.
c) El uso de los formatos recogidos y aceptados por la Norma Técnica de Interoperabilidad de Catálogo de Estándares.
d) La vinculación indisoluble de los documentos con sus firmas electrónicas asociadas cuando estas se requieran. La captura y custodia de firmas electrónicas se atendrá a los procedimientos establecidos por el órgano que ejerce la dirección de los sistemas de las tecnologías y la información en la materia[9].

En el momento de captura del documento en el sistema que se haya determinado, deberán informarse los siguientes metadatos mínimos obligatorios para el intercambio según establece la NTI de documento electrónico:

Metadato	Asignación en el momento de captura	Asignación en cualquier momento
Versión NTI	√	
Identificador	√	
Órgano	√	
Fecha de captura	√	
Origen	√	
Estado de elaboración	√	
Formato	√	

[9] Según el Procedimiento de uso de la firma electrónica longeva o de larga duración en los Sistemas de Información y Telecomunicaciones del Ministerio de Defensa y la Orden DEF/2594/2014, de 16 de diciembre, por la que se establece el sistema de utilización del código seguro de verificación de documentos electrónicos del Ministerio de Defensa

Metadato	Asignación en el momento de captura	Asignación en cualquier momento
Tipo documental		√
Tipo de firma	√	
Si el valor tipo de firma es CSV[10]:		
Valor CSV	√	
Definición generación CSV	√	
Si se trata de una copia de documento:		
Identificador del documento origen u Origen de la copia	√	

Igualmente, en el momento de creación o apertura de un expediente electrónico deberán informarse los siguientes metadatos obligatorios para el intercambio según la NTI de expediente electrónico:

Metadato	Asignación en el momento de captura	Asignación en cualquier momento
Versión NTI	√	
Identificador	√	
Órgano	√	
Fecha de apertura expediente	√	
Clasificación	√	
Estado		√
Interesado		√
Tipo de firma	√	
Si el valor Tipo de firma es CSV:		
Valor CSV	√	
Definición generación CSV	√	

La captura de un documento electrónico puede venir precedida por un proceso de digitalización y/o un proceso de conversión de formato que debe adecuarse a los requerimientos establecidos por las Normas Técnicas de Interoperabilidad y a la normativa interna desarrollada al respecto por el Ministerio de Defensa. Cuando por cual-

[10] CSV: código seguro de verificación.

quier circunstancia del trámite, los documentos se presentasen en papel, se deberán digitalizar lo antes posible de forma segura siguiendo el procedimiento de digitalización establecido en el Departamento[11].

Las reglas específicas aplicables a la creación y captura de documentos electrónicos y los metadatos relativos a los mismos deberán quedar recogidas en las instrucciones, guías y procedimientos que rigen los procesos de aquellos ámbitos de actividad, entornos de trabajo o tipologías de documentos que lo requieran.

4.4. REGISTRO ELECTRÓNICO

El Registro Electrónico del Ministerio de Defensa se adaptará a lo establecido en la LPAC y en la regulación del Ministerio de Defensa en cuanto a condiciones para la presentación de documentos.

La recepción de los documentos electrónicos en el Ministerio de Defensa se podrá realizar a través de:

a) El registro electrónico del Ministerio de Defensa y sus subregistros, así como en los restantes registros electrónicos de cualquiera de los sujetos a los que se refiere el artículo 2.1. de la LPAC.
b) Los registros o subregistros electrónicos del Ministerio de Defensa que existan o puedan existir fuera del territorio nacional.
c) El Sistema de Interconexión de Registros (SIR), que permite la digitalización e intercambio de documentos electrónicos con registros de otras Administraciones Públicas.
d) Las oficinas de Correos, en la forma que reglamentariamente se establezca.
e) Cualquier otro que establezcan las disposiciones vigentes.

Los registros electrónicos deberán ser interoperables para garantizar la interconexión y la transmisión telemática de los asientos registrales y de los documentos que se presenten en cualquiera de los registros y subregistros, siguiendo las directrices marcadas por la NTI de Modelo de Intercambio de Asientos Registrales entre Unidades.

[11] Manual de digitalización para fondos bibliográficos, documentación de archivo y fondos museográficos (http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=51506).

En el registro deberá realizarse el correspondiente asiento registral de toda la documentación que sea presentada o recibida, así como el registro de la salida de los documentos oficiales dirigidos a otros órganos o particulares. Los asientos deberán respetar el orden temporal de entrada y salida de los documentos y deberán indicar la fecha del día en que se produzcan.

Los sistemas de registro del Ministerio de Defensa deberán dejar constancia de la relación entre los documentos electrónicos registrados y el recibo de registro generado por ellos; deberán garantizar la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra. El recibo de registro, incluirá, además de los metadatos obligatorios de cualquier documento electrónico, los siguientes:

Metadato	Descripción
Registro. Número Registro	Número de registro del documento
Registro. Fecha Registro	Fecha de registro del documento
Registro. Tipo Registro	Identificación del libro de registro, para el cual el número de registro arriba indicado debe ser único
Registro. Asunto	Asunto asociado al asiento registral

El tratamiento y práctica de las notificaciones por parte del Ministerio deberá adaptarse a la LPAC. Se practicarán preferentemente por medios electrónicos y la acreditación de la notificación efectuada deberá incorporarse al expediente correspondiente, asignándole los metadatos pertinentes.

En lo que respecta a la documentación clasificada, el sistema de registro en España está constituido por el Registro Central y todos los órganos de control autorizados por la Autoridad Nacional de Seguridad para la protección de la información clasificada, o creados en el ámbito de la Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO). Este sistema es parte fundamental de la infraestructura nacional de protección de esta información y está estructurado jerárquicamente

conforme a un esquema de responsabilidad establecido en la Norma NS/01 de seguridad para la protección de la información clasificada.

4.4.1. Digitalización en el punto de registro

En los casos que la recepción de documentos en el registro de entrada se realice en soporte papel, se procederá a su digitalización, devolviéndose los originales al interesado, sin perjuicio de los supuestos que una norma determine sobre la custodia de los mismos por parte del Ministerio de Defensa, o se trate de objetos o documentos en soportes no susceptibles de digitalización.

El proceso de digitalización se realizará cumpliendo las especificaciones de las Normas Técnicas de Interoperabilidad de Digitalización y de Documento Electrónico, y en particular, el protocolo de digitalización del Departamento.

El Ministerio de Defensa podrá reglamentar la obligación de presentar determinados documentos por medios electrónicos para ciertos procedimientos y colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

En la fase de transición hacia la aplicación de la LPAC, en la que los expedientes abiertos contengan documentos en papel, las Unidades del Ministerio de Defensa deberán valorar la rentabilidad de aplicar un proceso de digitalización para convertir dichos expedientes en electrónicos.

5. Procesos de clasificación documental y descripción

5.1. CONCEPTO Y PROPÓSITO DE LA CLASIFICACIÓN DOCUMENTAL

La clasificación consiste en la identificación y estructuración sistemática en categorías, de todos los documentos del Ministerio de Defensa de acuerdo a las funciones y actividades que los originan.

Atendiendo a lo establecido en el RAM, los documentos del Ministerio de Defensa y sus agrupaciones serán clasificados con un criterio orgánico funcional que tendrá como base el principio de procedencia. Para los documentos electrónicos, la procedencia orgánica será informada a través de los metadatos relativos a los agentes productores y la procedencia funcional a través de los metadatos relativos a la clasificación documental. El anexo 4 presenta un esquema de funciones que servirá como base para el desarrollo del cuadro de clasificación.

Como regla general, la clasificación se aplicará al nivel de agrupación de *serie documental*, que se describe en el punto 5.3 de esta política.

El propósito de la clasificación documental será:

a) Contextualizar y establecer vínculos entre los documentos de forma que representen la actividad de la organización.

b) Mantener la consistencia en las denominaciones de los documentos.
c) Tomar decisiones relativas al acceso, seguridad, la distribución de responsabilidades, la conservación, etc. en base a categorías.
d) Organizar los repositorios corporativos y los archivos físicos y electrónicos.
e) Permitir la herencia de metadatos desde las categorías más genéricas a las más específicas.
f) Ayudar a la recuperación y a la navegación por conjuntos de documentos.

5.2. INSTRUMENTOS DE CLASIFICACIÓN

Podrán utilizarse en el Departamento, los siguientes instrumentos de clasificación:

a) Cuadro de clasificación documental: será de carácter corporativo y estructurará las funciones y actividades del Ministerio de Defensa con el objeto de aportar el contexto de procedencia funcional de los documentos[12]. El Ministerio de Defensa desarrollará un cuadro de clasificación aplicable a la gestión de los documentos electrónicos, basado en el análisis documental y en los cuadros empleados en otros organismos de defensa de otros países, cumpliendo así las directrices establecidas en el artículo 21 del ENI. El cuadro de clasificación deberá implementarse de forma que pueda dar servicio a los sistemas de información en los que se gestionan los documentos electrónicos desde el momento mismo de su configuración. Para su implementación en un modelo de metadatos multientidad se emplearán preferiblemente los metadatos y valores estándares para:

e-EMGDE 0 Tipo de entidad = Actividad e-EMGDE 1 Categoría= *Función marco, función, actividad, acción*

Se establecerá un procedimiento específico de mantenimiento, actualización y aprobación del cuadro de clasificación.

[12] Las buenas prácticas y los estándares de gestión documental recomiendan emplear preferiblemente sistemas funcionales por ser más persistentes y comprensibles a lo largo del tiempo que los sistemas basados exclusivamente en la procedencia orgánica.

b) **SIA**: el Sistema de Información Administrativa (SIA) es el inventario de información administrativa de la Administración General del Estado, reglado por el artículo 9 del Esquema Nacional de Interoperabilidad y actualizado de forma corresponsable por todos los Organismos participantes. Contiene la relación de procedimientos y servicios de la AGE y las diferentes Administraciones Públicas participantes. El SIA se podrá emplear, adicionalmente, para informar de los metadatos de clasificación para los expedientes administrativos del Ministerio de Defensa.

5.3. NIVELES DE AGRUPACIÓN DOCUMENTAL

Los documentos se agrupan en distintos niveles, lo que facilita la toma de decisiones y adopción de políticas homogéneas. Los niveles de clasificación documental, que se definen en el esquema de metadatos e-EMGDE y en los estándares internacionales, son: grupo de fondos, fondo, serie (de expedientes, de agregaciones documentales y de documentos simples), expediente, agregación documental y documento simple.

a) **Grupo de fondos**: conjunto de fondos que están vinculados por pertenecer a una jurisdicción o sector específico, por realizar unas funciones similares o por razones de custodia. En el Ministerio de Defensa se considerará grupo de fondos, a efectos de su tratamiento electrónico, por ejemplo a los afectados por la clasificación de secretos oficiales y que requieren ser tratados en sistemas de información específicos con niveles máximos de seguridad y custodia.

b) **Fondo**: conjunto de documentos producidos o recibidos por un órgano o sujeto en el ejercicio de sus funciones o actividades y que aglutina un conjunto de series de la misma procedencia institucional. La conformación de los fondos en los entornos de gestión de documentos electrónicos se atendrá a la práctica establecida por el Reglamento de Archivos Militares y su aplicación al Sistema Archivístico de la Defensa.

c) **Serie documental**: se entiende por serie documental el conjunto de unidades documentales de estructura y contenido homogéneos recibidas o producidas por un mismo órgano o sujeto productor en el ejercicio de cada una de sus funciones específicas.

Las series documentales del Ministerio de Defensa, podrán ser de tres tipos:

1.º Series de expedientes: aquellas que cumplen las características de la definición de expediente de la LPAC y que corresponden a procedimientos reglados.
2.º Series de agregaciones documentales: aquellas que atienden a la definición del e-EMGDE y que podrán ser, en el entorno electrónico, carpetas u otros objetos de información agrupadores que engloban documentos producidos al margen de cualquier procedimiento reglado.
3.º Series de documentos simples: son las formadas por documentos unitarios y definitivos.

Toda la documentación electrónica que se gestione de acuerdo a esta política deberá tener identificada y asignada el tipo y la denominación de la serie documental a la que pertenece, según el análisis documental.

d) Expediente: la definición y requisitos del expediente administrativo quedan establecidos en la LPAC art 70 como «conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla».
Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.
Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad, y se enviará completo, foliado, autenticado y acompañado de un índice, asimismo autenticado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

No formará parte del expediente administrativo la información que tenga carácter auxiliar o de apoyo.
Los expedientes pueden estar compuestos de elementos en soporte digital, analógico o incluso de objetos, formando expedientes híbridos. Para los documentos y objetos no digitalizables se mantendrá siempre la relación con el expediente (a través de las referencias cruzadas necesarias) de forma que se permita recuperar la totalidad del mismo.
Se considera expediente, dentro del ámbito de esta política, tanto a los administrativos regulados por la Ley 39/2015, como a cualquier otro tipo de expediente regulado por procedimientos particulares del ámbito de la Defensa tales como los derivados de la aplicación de la justicia militar, la gestión sanitaria en el ámbito del departamento, etc.

e) **Agregación de documentos**: agrupación de documentos creada al margen de un procedimiento reglado. A modo de ejemplo en el Ministerio de Defensa se considerarán bajo este concepto los conjuntos fotográficos, proyectos I+D, memorias, colecciones, etc.
Las agregaciones de documentos del Ministerio de Defensa cumplirán los mismos requerimientos que se aplican a los expedientes electrónicos cuando así se determine en el análisis documental.

f) **Documento simple**: unidad mínima de los niveles agrupación documental. En el Ministerio de Defensa, y a efectos de su gestión electrónica según esta política, se tratará siempre de un objeto único al que pueden aplicar los estados de elaboración previstos en el metadatos obligatorio e-EMGDE 20 - Estado de elaboración:

EE01 (Original)
EE02 (Copia electrónica auténtica con cambio de formato)
EE03 (Copia electrónica auténtica de documento papel)
EE04 (Copia electrónica parcial auténtica)
EE99 (Otros)

5.4. APLICACIÓN DE LA CLASIFICACIÓN DOCUMENTAL

La clasificación documental, según el cuadro de clasificación o el SIA, se puede aplicar a cualquier nivel de agrupación.

El nivel de agrupación documental que se describe y clasifica, se indicará en la entidad eEGMDE0 = documento, con el valor correspondiente del

metadato obligatorio e-EMGDE 1 Categoría = Grupo de fondos, fondo, serie documental, agregación documental, expediente, documento simple.

Obligatoriamente se asignará la clasificación a todas las series documentales identificadas en el Ministerio de Defensa y, adicionalmente, de la clasificación SIA según el procedimiento administrativo que corresponda. Para ello se emplearán los metadatos:

e-EMGDE 22.1 Código de Clasificación e-EMGDE 22.2 Denominación de la clase e-EMGDE 22.3 Tipo de clasificación * (SIA/funcional)

Para las series de expedientes, los metadatos de clasificación se deberán capturar obligatoriamente en el momento de la apertura de los mismos. En los otros tipos de series documentales (de agregaciones documentales y documentos simples) se podrán aplicar desde el momento de su configuración, o en procesos posteriores, como puede ser la transferencia desde los sistemas de origen al archivo único electrónico.

Se optará preferiblemente por implementaciones técnicas que permitan la herencia de los metadatos de clasificación desde el nivel de serie documental a todos los expedientes o agregaciones y por ende a los documentos contenidos en los mismos.

5.5. DESCRIPCIÓN

Describir implica representar los documentos y sus niveles de agrupación mediante información estructurada en metadatos que servirán para su localización y uso a lo largo de su ciclo de vida.

El uso de metadatos de descripción adicionales a los obligatoriamente establecidos en el proceso de captura, será facultativo y podrá producirse en cualquier momento del ciclo de vida de los expedientes y documentos. Este aspecto se determinará en función de las necesidades de recuperación identificadas en el análisis documental.

En la descripción se podrán utilizar taxonomías y vocabularios controlados geográficos, temáticos u otros, que faciliten la búsqueda y recuperación.

Los metadatos a desarrollar en el e-EMMDEF a partir del esquema e-EMGDE para este propósito serán:

e-EMGDE5 Descripción e-EMGDE12 Puntos de acceso

Para la descripción de los documentos y expedientes se podrá tener en cuenta el Tesauro del Ministerio de Defensa.

6. Procesos de calificación, conservación, transferencia y eliminación

6.1. CALIFICACIÓN

6.1.1. Concepto y propósito de la calificación

La calificación es el proceso documental que comprende la determinación de los documentos esenciales, la valoración de los documentos para el establecimiento de los plazos de conservación, acciones de transferencia o eliminación, régimen de acceso y el dictamen de la autoridad calificadora.

La calificación se aplicará sobre cualquier documento que haya sido creado o recibido en el marco de las competencias que el Ministerio de Defensa tiene encomendadas.

6.1.2. Documentos esenciales

Son aquellos documentos indispensables y vitales para la continuidad digital y que, en caso de desastre o emergencia, permitirán que el Ministerio de Defensa pueda alcanzar sus objetivos, cumplir con sus obligaciones diarias de servicio y respetar la legalidad vigente y los derechos de las personas.

La determinación de los documentos esenciales se realizará en el contexto del cumplimiento de los requerimientos establecidos en el Esquema Nacional de Seguridad y aplicación de la política de gestión de riesgos del Ministerio de Defensa. Este trabajo puede estar contemplado en el análisis documental previo a la implementación de los sistemas de información en que se vayan a gestionar los documentos electrónicos.

Los documentos esenciales deberán ser incluidos en el Plan de Continuidad Digital y Recuperación ante Desastres del Ministerio de Defensa. Se deberán adoptar las medidas necesarias para asegurar su confidencialidad, integridad, disponibilidad y autenticidad.

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

a) Informan de las directrices, estrategias y planificación de la organización.
b) Recogen derechos de la organización, singularmente los relativos a convenios y documentos de propiedad.
c) Recogen información sobre los edificios, instalaciones y sistemas de la organización.
d) Dejan constancia de los acuerdos y resoluciones de los órganos de gobierno de la organización, tanto colegiados como unipersonales.

La gestión de los documentos calificados como esenciales requerirá la obtención de una réplica según lo dispuesto en el procedimiento de copiado auténtico de documentos a que se refiere el anexo 2 y que se garanticen las adecuadas condiciones de protección y conservación.

Cuando exista un documento esencial en soporte papel, forme o no parte de un expediente o agregación documental y se realice copia electrónica auténtica del mismo, el original permanecerá en su lugar de origen y se someterá a los procedimientos de valoración correspondientes a su serie.

6.1.3. Valoración y dictamen

La valoración documental es el proceso de estudio y análisis de las características de las series documentales del Departamento y que

da como resultado un dictamen en el que se establecen los plazos de conservación, transferencia y acceso. Dicho análisis debería realizarse con carácter previo a la captura y/o creación de los mismos en los sistemas de información en que se van a gestionar durante todo su ciclo de vida.

Como regla general, las propuestas de transferencia, régimen de acceso y conservación o eliminación, se realizarán para el nivel de agrupación de serie documental y se heredarán a los niveles inferiores hasta llegar al documento propiamente dicho. Podrán aplicarse excepciones cuando las características de la documentación así lo aconsejen.

En la determinación de los plazos de conservación deberán incluirse la valoración respecto a la conservación de las firmas y los metadatos asociados a los documentos.

Al igual que en el soporte papel, los valores primarios y secundarios de los documentos, a efectos de conservación, se determinarán teniendo en cuenta el marco reglamentario, las necesidades de gestión y de rendición de cuentas, el riesgo para la institución y el valor histórico.

Se entiende por valor primario de un documento, el de la finalidad inmediata por la que fue producido o creado. Entre otros, los valores primarios pueden ser:

a) Administrativo: el que posee un documento para la administración de origen o aquella que le sucede, como testimonio de sus funciones y actividades.
b) Contable: el que tienen los documentos que pueden servir de explicación o justificación de operaciones destinadas al control presupuestario.
c) Fiscal: el de los documentos que pueden ser testimonio de cumplimiento de obligaciones tributarias.
d) Jurídico: el que se deriva de derechos u obligaciones legales.
e) Legal: el que pueden tener todos los documentos que sirvan de testimonio ante la ley.

Se entiende por valor secundario el que obedece a otras motivaciones que no son la propia finalidad del documento y que adquiere

o puede adquirir con el paso del tiempo. Estos valores secundarios pueden ser:

a) Informativos: que sirven de referencia para la elaboración o reconstrucción de cualquier actividad del Departamento y que pueden ser testimonio para la memoria colectiva.
b) Históricos: que poseen los documentos como fuentes primarias de la historia.

Con carácter general y siguiendo las directrices del Ministerio de Educación y Cultura y Deporte, para la valoración de los documentos del Ministerio de Defensa, se deberán tener en cuenta los siguientes criterios:

a) De procedencia; primar las series documentales producidas por los órganos y unidades que ocupan una posición más elevada en la organización jerárquica del departamento.
b) Funcional; primar las series producidas en el ejercicio de funciones propias y específicas de cada órgano y unidad.
c) Producción; primar las series producidas por órganos y unidades que realizan el procedimiento completo.
d) Diplomático; valorar únicamente los documentos originales, terminados y validados y las copias solo en ausencia del original.
e) De utilización; primar las series y documentos que durante su etapa activa y semiactiva (según el ciclo de vida) hayan sido objeto de demanda frecuente y aquellos que por su origen, período cronológico que abarcan o contenido, se espera y prevé que sean objeto de consulta por parte de usuarios potenciales.

El procedimiento de valoración se establece en el art. 13 del RAM y comprenderá las propuestas de valoración por parte de las subcomisiones nombradas a tal efecto por el Ministerio de Defensa, el dictamen preceptivo y vinculante por parte de la Comisión Calificadora de Documentos de la Defensa y, cuando corresponda, el de la Comisión Superior Calificadora de Documentos del Ministerio de Educación, Cultura y Deporte, su aprobación y publicación. El trámite se realizará de forma automatizada dando lugar a su correspondiente expediente electrónico de valoración.

El dictamen resultante del proceso de valoración determinará

a) Los plazos de conservación: permanente o temporal.
b) Las acciones a llevar a cabo: transferencia (analizada en el apartado 6.3 de esta política) y/o eliminación total o parcial. La selección del criterio para la eliminación parcial puede basarse en distintos métodos de muestreo.
c) El régimen de acceso: analizado en el apartado 7 de esta política.

Los dictámenes de valoración de las series tomarán como referente los emitidos por los órganos calificadores de otros Departamentos y en especial de la Comisión Superior Calificadora de Documentos Administrativos del Ministerio de Educación Cultura y Deporte.

Los sistemas electrónicos de gestión documental, en función del dictamen de valoración, permitirán el expurgo en los mismos sistemas, los cambios de almacenamiento, la migración entre sistemas, la transferencia de responsabilidad, etc.

Con los resultados del proceso de valoración se elaborará un calendario de conservación. Este instrumento contiene el cuadro de series documentales y las acciones dictaminadas en lo concerniente al tiempo de permanencia, plazos de transferencia y condiciones de eliminación de los documentos. El calendario de conservación del Ministerio de Defensa será aplicable tanto a la gestión de los documentos en soporte físico como electrónico.

Como criterio general, y siguiendo las pautas establecidas en la política de retención y disposición de la OTAN[13], se considerará documentación de conservación permanente toda aquella relacionada con:

a) Las políticas, decisiones, eventos, consultas importantes, misiones y actividades.
b) La estructura y evolución del Ministerio de Defensa.
c) La situación legal y financiera, las obligaciones y responsabilidades del Ministerio.
d) El impacto de las decisiones del Departamento sobre los derechos, la salud y la seguridad de su personal y / u otras personas.

[13] Policy on the Retention and Disposition of NATO Information. 2009 (http://www.nato.int/nato_static/assets/pdf/pdf_archives/20120327_C-M_2009_0021_INV-Retention_Dispo_of_NATO_Inf.pdf).

e) El impacto sobre el medio físico.
f) Los informes de carácter público que faciliten el conocimiento y comprensión de los propósitos, principios y logros del Ministerio de Defensa.

La documentación de valor temporal, llevará definido el número de años que debe conservarse y las acciones que deban realizarse con la misma para su conservación en los sistemas electrónicos hasta el fin del plazo dictaminado.

Los metadatos a desarrollar en el e-EMMDEF para el proceso de calificación dentro del sistema o sistemas en que se gestiona el ciclo de vida de los documentos, se basarán en los previstos en el e-EMGDE:

e-EMGDE 13 – Calificación
- e-EMGDE 13.1 – Valoración
  - e-EMGDE 13.1.1 – Valor primario
    - e-EMGDE 13.1.1.1 – Tipo de valor
    - e-EMGDE 13.1.1.2 – Plazo
  - e-EMGDE 13.1.2 – Valor secundario
- e-EMGDE 13.2 – Dictamen
  - e-EMGDE 13.2.1 - Tipo de dictamen
  - e-EMGDE 13.2.2 - Acción dictaminada
  - e-EMGDE 13.2.3 – Plazo de ejecución de la acción dictaminada
- EMGDE 13.4 – Documento esencial

6.2. CONSERVACIÓN

La conservación se define como el conjunto de procesos y operaciones que tienen como objetivo garantizar el adecuado mantenimiento de los documentos a lo largo del tiempo. La creación y captura-de un documento implica, ya de por sí, la intención de almacenarlo durante un tiempo determinado. Todos los documentos generados por las administraciones públicas son, o pueden ser, patrimonio documental, según la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (LPHE).

Los documentos electrónicos del Ministerio de Defensa deberán conservarse almacenados en las condiciones apropiadas de soporte y formato, que garanticen su disponibilidad, fiabilidad, autenticidad

y conservación a lo largo de toda su existencia, especialmente en el caso de los documentos identificados para su conservación permanente.

Para la conservación de los documentos electrónicos se aplicarán los metadatos específicos de preservación PREMIS cuya equivalencia con el e-EMGDE se incluye en el Anexo 5 de esta política.

Se desarrollará un plan de preservación digital siguiendo las orientaciones definidas como anexo 5 de esta política, que contemple estrategias de almacenamiento digital tales como:

a) Sistemas de copias de seguridad para prevenir la pérdida de documentos por fallos en los sistemas.
b) Conversión, que implica cambio de formato garantizando la información primaria, con el objeto de prevenir el daño físico de los soportes.
c) Migración para abordar la obsolescencia del hardware y software que pueda afectar a la legibilidad de los documentos electrónicos almacenados.

La planificación de conservación de documentos electrónicos del Ministerio de Defensa, dependerá de su capacidad para mantener la accesibilidad, integridad y autenticidad de los mismos a lo largo del tiempo, y de la relación coste-beneficio y deberá contemplar tanto los documentos electrónicos como sus metadatos asociados para garantizar que ambos van a ser accesibles y utilizables durante todo su plazo de conservación.

Para garantizar el uso de los documentos electrónicos a lo largo del tiempo deben eliminarse las restricciones que puedan existir sobre los mismos después de un periodo determinado, como:

a) Uso de cifrado/encriptado.
b) Uso de contraseña.
c) Aplicación de derechos digitales que restrinjan el acceso o limiten la vida útil de un registro.

El sistema o sistemas de gestión de documentos electrónicos del Ministerio que se determinen, deberán mantener en todo momento la trazabilidad de las acciones u operaciones realizadas sobre los mismos en materia de conservación.

La documentación clasificada se custodiará en contenedores separados manteniendo en todo momento una estricta compartimentación dentro de cada tipo de la información en función de su grado de clasificación, según las Normas de la Autoridad Nacional de Seguridad para la protección de la información clasificada. Podrá ser almacenada en sistemas de información y comunicaciones y en soportes informáticos, siempre que el sistema se encuentre acreditado y esté autorizado por la autoridad competente, de forma que en su protección se garanticen medidas de seguridad tan rigurosas como para los documentos sobre papel u otros soportes físicos. Estos sistemas han de asegurar igualmente, de forma física o lógica, la compartimentación indicada en el párrafo anterior, así como cuanto se indica en la normativa específica sobre modos seguros de operación de los sistemas.

Todos los soportes removibles de almacenamiento informático (discos duros, disquetes, CD-ROM, «pendrives», etc.) que contengan información clasificada tienen la consideración de documentos, por lo que deberán estar debidamente identificados, marcados y registrados. La clasificación de seguridad del soporte indicará la más alta clasificación de la información que alguna vez haya sido almacenada en el mismo, a no ser que la misma fuera eliminada con algún procedimiento aprobado por la autoridad competente.

Para la información almacenada en forma de expedientes o en soporte informático que contengan más de un grado de clasificación, se aplicarán las medidas de protección correspondientes al mayor grado de clasificación de la información contenida, por el principio de agregación según las Normas de la Autoridad Nacional de Seguridad para la protección de la información clasificada.

La conservación de los documentos en soporte papel se regirá por lo establecido en el *Capítulo IX. De la conservación de los documentos* del RAM.

6.3. TRANSFERENCIA

La transferencia es el procedimiento habitual de ingreso de fondos documentales en un archivo o repositorio, mediante el traslado de series o fracciones de serie una vez han cumplido el plazo de permanencia fijado en la valoración documental. Su propósito es facilitar el

paso de los documentos en sus fases de vida de manera que puedan recibir el tratamiento adecuado en cada una de ellas. En el ámbito electrónico, se materializa en el cambio de la custodia y de la responsabilidad, con o sin cambio de repositorio.

La transferencia de documentos electrónicos del Ministerio de Defensa, estará sujeta al procedimiento que se establezca, en el marco del Sistema Archivístico de la Defensa y de los requerimientos de la Política de la Seguridad de la Información y las Comunicaciones del Departamento.

Ateniéndose a lo establecido en el RAM, y en el plazo dictaminado para la acción resultante del proceso de valoración, se llevará a cabo la transferencia de la responsabilidad al Órgano responsable del Sistema Archivístico de la Defensa. Todo cambio de repositorio deberá estar definido y controlado en el sistema de información en que se gestionan los documentos electrónicos, a partir de lo dispuesto en los calendarios de conservación.

Conforme a lo establecido en las NTI de documento y expediente electrónico y en tanto no se publique una norma específica de transferencias, el órgano o entidad que transfiere es la responsable de verificar la autenticidad e integridad de lo transferido en el momento del intercambio, mediante la firma electrónica de los índices de los expedientes y de los documentos electrónicos.

Los documentos que se transfieran deben ir asociados a sus metadatos y firmas correspondientes para permitir su identificación, autenticidad y conservación. Serán acompañados de indicaciones respecto a procedimientos:

a) De uso y acceso.
b) De seguridad para prevenir, corregir y descubrir pérdidas de información o alteración de documentos.
c) De conservación en relación al deterioro de soportes y obsolescencia tecnológica.

Se desarrollará un protocolo de transferencia en el que se contemple la necesidad de:

1.º Adaptar los documentos a un formato longevo, incluyendo las posibles migraciones o cambios de formato que se prevean necesarios.

2.º Añadir las firmas y la información necesaria para su verificación y validación así como los sellos de tiempo que garanticen la conservación a largo plazo de las mismas, si fuera necesario.
3.º Revisar la documentación y actualizar y completar los metadatos mínimos necesarios para la transferencia con cambio de custodia.
4.º Disponer de mecanismos de bloqueo para aquellos documentos o expedientes que, por determinados motivos, deban exceptuarse de la aplicación de las reglas generales.

En los sistemas deberá quedar constancia de la remisión de expedientes por el órgano o aplicación emisora y de su recepción en el destino.

En caso de que la transferencia suponga una duplicación de documentos, el órgano remitente, una vez obtenida la conformidad del responsable que los ha recibido, deberá proceder al borrado seguro de sus ejemplares, como se indica en el apartado 6.4 de esta política.

En el caso de remisión de expedientes híbridos, se deberá acompañar una relación de entrega de los mismos y deberá establecerse una referencia cruzada que permita la vinculación de todas las partes del expediente al objeto de su recuperación completa.

Cuando la transferencia se realice en soportes físicos, tales como discos duros o similares, deberán tenerse presentes las medidas de seguridad en el transporte y de integridad de los soportes que se recogen en la normativa de seguridad del Departamento y las establecidas por la Autoridad Nacional de Seguridad en las Normas para la protección de la información clasificada.

La documentación producida por organismos o unidades del Ministerio de Defensa ubicadas fuera del territorio nacional, también será objeto de transferencia reglada a los archivos correspondientes. Cuando esta documentación no se gestione desde su origen en los sistemas corporativos determinados para la gestión y el archivo de documentos, se deberá transferir en los plazos dictaminados, la custodia al archivo único electrónico y la responsabilidad al órgano responsable del Sistema Archivístico de la Defensa.

Todos los documentos de conservación permanente deberán ser transferidos al archivo electrónico único que se determine como sistema de preservación digital a largo plazo.

Los documentos de conservación temporal deberán ser eliminados en sistemas que dispongan de las funcionalidades necesarias para proceder a su destrucción controlada en el plazo previsto. Si los sistemas en que se gestionan en origen no dispusieran de dichas funcionalidades, la custodia y responsabilidad deberá ser transferida al órgano Responsable del SAD.

De las transferencias realizadas en el Ministerio de Defensa deberá quedar constancia de los movimientos y eventos producidos, mediante metadatos de trazabilidad de las acciones realizadas. Los metadatos a desarrollar en el e-EMMDEF partirán de los siguientes previstos en el e-EMGDE:

e-EMGDE 13.3 –Transferencia
e-EMGDE 13.3.1 – Fase de archivo
e-EMGDE 13.3.2 – Plazo de transferencia

La transferencia de documentos en soporte papel entre los distintos archivos del Ministerio de Defensa se regirá por lo establecido al respecto en el RAM.

6.4. DESTRUCCIÓN O ELIMINACIÓN

El concepto de destrucción de documentos y la información que contienen, queda definido en el artículo 27 de la Instrucción 64/2015, de 7 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas de seguridad de la información para la elaboración, clasificación, cesión, distribución y destrucción de información del Ministerio de Defensa:

a) Se entiende como destrucción de la información, la eliminación de todos y cada uno de los elementos tangibles que le den soporte. Se considerará que no se ha destruido la información si esta puede encontrarse en algún elemento tangible. El proceso de destrucción implicará que esta se elimine de todos los documentos o sistemas de información y comunicaciones en los que se encuentre.

b) La destrucción de los elementos tangibles que dan soporte a la información clasificada, se establece en los artículos 28 al 32 del Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales así como en la normativa específica de desarrollo o de aplicación de la seguridad de la información en los documentos, seguridad de la información en los sistemas de información y comunicaciones y seguridad de la información en poder de las empresas.
c) En ningún caso se podrá destruir información en tanto subsista en ella un valor probatorio de derechos y obligaciones de las personas físicas o jurídicas o no hayan transcurrido los plazos que la legislación establezca para su conservación, de acuerdo con lo dispuesto en la regulación relativa a la conservación de la información en el Sistema Archivístico de la Defensa.

La documentación electrónica a destruir, sujeta a esta política, será la que previamente se haya dictaminado en el proceso de valoración por los órganos competentes y requerirá:

1.º El dictamen preceptivo de la Comisión Calificadora de Documentos de la Defensa y, cuando proceda, la resolución de la Comisión Superior Calificadora de Documentos Administrativos.
2.º Un proceso de destrucción o eliminación segura de documentación electrónica y soportes informáticos que se atenga a las instrucciones de seguridad de la información del Ministerio de Defensa y a la normativa de seguridad para la destrucción de la documentación clasificada de la Autoridad Nacional de Seguridad para la protección de la información clasificada.
3.º El trámite del expediente de eliminación en soporte electrónico, dejando traza de las acciones realizadas.

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

a) Destrucción de información como última fase de un procedimiento reglado de eliminación y destrucción, realizado con las formalidades del 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 en sus artículos 7 y 8. Este hecho figurará en los dictámenes correspondientes a la serie documental.

b) Cambio de soporte o formato como consecuencia de la 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.
c) 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, como ya se ha expuesto en el apartado 6.3 de esta política.

En los dos últimos supuestos, y siempre que se realicen copias auténticas con/sin cambio de formato con las exigencias del ENI, se aplicará dicho Real Decreto y las Normas Técnicas de Interoperabilidad que lo desarrollan.

Los metadatos a desarrollar para el control del proceso de eliminación o destrucción se basarán en los previstos en el e-EMGDE:

e-EMGDE 21 – Trazabilidad.
- e-EMGDE 21.1 - Acción: «Destruye» o «Elimina»
  - e-EMGDE 21.1.1 - Fecha de la acción.
  - e-EMGDE 21.1.2 - Entidad de la acción.
- e-EMGDE 21.2 - Motivo reglado.
- e-EMGDE 21.3 - Usuario de la acción.

Los aspectos técnicos de la destrucción de la información quedarán determinados por las normas de seguridad de la información en los documentos, normativa específica de desarrollo del Ministerio de Defensa, y de la Autoridad Nacional de Seguridad para la protección de la información clasificada.

Como conclusión, la aplicación de la destrucción de los documentos deberá contemplar que:

a) Solo se destruirá la documentación valorada previamente.
b) La destrucción siempre debe haber sido autorizada.
c) Los documentos y expedientes en trámite o sujetos a litigios o investigaciones posteriores a su cierre, no deberán destruirse.
d) Deberá realizarse preservando la confidencialidad de cualquier información que contengan.
e) Incluye la destrucción de todas las copias que pudieran existir, incluidas copias de seguridad electrónica y copias de conservación.

En el caso de destrucción inmediata y de emergencia de documentos clasificados o no clasificados, esta deberá ser comunicada y documentada, a la mayor brevedad posible, a los responsables del SAD, de forma que se contabilice y regularice el proceso de destrucción una vez cesadas las circunstancias excepcionales que lo motivaron.

7. Acceso

7.1. ACCESO A LOS DOCUMENTOS ELECTRÓNICOS

Se define acceso como el derecho, modo y medios de localizar, usar y recuperar los documentos electrónicos que cumplen con los requerimientos establecidos en la PGDE-MINISDEF.

El derecho de acceso a los documentos electrónicos está regulado por la legislación vigente que establece las condiciones y/o restricciones aplicables según las características de los mismos y queda recogido en el artículo 105.b) de la Constitución Española que se desarrolla en la LTAIP.

Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de la LTAIP y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

El art. 13 d) LPAC, establece que las personas, en sus relaciones con las administraciones públicas, son titulares del derecho al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la LTAIP y el resto del ordenamiento jurídico.

El derecho de acceso a los documentos podrá ser limitado en base a los supuestos previstos en el artículo 105.b) de la Constitución Española y en los artículos 14 y 15 de la LTAIP. La codificación de estas

restricciones a efectos de cumplimentación del esquema de metadatos se recoge en el anexo 6 de esta política.

Además, será vinculante para los documentos del Ministerio de Defensa, el cuerpo normativo sobre secretos oficiales que se inicia con Ley 9/1968, de 5 de abril, sobre Secretos Oficiales (LSO), desarrollada mediante el Decreto 242/1969, de 20 de febrero, y modificada por la Ley 48/1978, de 7 de octubre. En virtud de esta normativa, se consideran «materias clasificadas» los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la Seguridad y Defensa del Estado.

En el anexo 6 se aportan los valores de los niveles de clasificación de seguridad y sus equivalencias en el ámbito internacional de la defensa.

El acceso a los documentos electrónicos se realizará por medio de los sistemas y tecnologías de la información y comunicaciones del Ministerio de Defensa en las que estos se gestionan o transmiten. Con el objeto de garantizar la protección adecuada, proporcionada y razonable de los documentos electrónicos del Ministerio de Defensa, asegurando la preservación de sus requisitos básicos de seguridad (confidencialidad, integridad y disponibilidad), será de aplicación lo establecido en la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa y en todas sus normas derivadas, así como lo establecido en las Normas de la Autoridad Nacional de Seguridad para la protección de la información clasificada.

7.2. RÉGIMEN DE ACCESO

7.2.1. Categorías de acceso

El régimen de acceso y de seguridad de los documentos electrónicos del Ministerio de Defensa está determinado en la clasificación que establece la normativa de seguridad de la información. A estos

efectos, los documentos electrónicos podrán pertenecer a una de las siguientes categorías:

a) Información no clasificada, dependiendo de su ámbito de distribución los documentos electrónicos podrán ser:

   1.º De uso oficial: aquellos cuya distribución esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo.
   2.º De uso público: aquellos cuya distribución NO esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo. Se conceptúan como documentos de uso público, los documentos electrónicos que queden sujetos al régimen de publicidad activa en cumplimiento de lo establecido en la LTAIP. Para dichos documentos deberá determinarse, cuando proceda, sus condiciones de reutilización.

b) Información clasificada, cualquier información o material respecto del cual se decida que requiere protección contra su divulgación o acceso no autorizados, por el daño o riesgo que esto supondría a los intereses del Estado, y al que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad. Los grados aplicables a los documentos electrónicos que formen parte de la información clasificada serán los establecidos en la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa:

   1.º Secreto (S), que se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello pudiera dar lugar a riesgos o perjuicios de la Seguridad y Defensa del Estado.
   2.º eservado (R), que se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a la Seguridad y Defensa del Estado.

3.º onfidencial (C) , que se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar el cumplimiento de su misión.
4.º ifusión limitada (DL), que se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

7.2.2. Documentos electrónicos no clasificados

El régimen de acceso a los documentos electrónicos no clasificados estará sujeto a la legislación vigente, y se les aplicarán las condiciones de acceso que les afecten tanto a los procedimientos en curso como a los finalizados.

Con carácter general, los documentos electrónicos, que constituyen patrimonio documental según el art. 49 de la LPHE y forman parte del SAD según el art.25 del RAM, una vez concluida su tramitación y registrados en el archivo electrónico único del Ministerio de Defensa, serán de libre consulta a no ser que afecten a materias clasificadas de acuerdo con la Ley 48/1978, de 7 de octubre, por la que se modifica la LSO, o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la defensa del Estado o la averiguación de los delitos.

El procedimiento para el acceso a los documentos se ajustará a lo establecido en el Capítulo IV «Procedimiento de acceso a documentos y archivos» 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[14].

[14] LPHE. Disposición adicional cuarta. Sistema Archivístico de la Defensa. *El Sistema Archivístico de la Defensa se rige por su normativa específica. No obstante, el régimen de acceso a los documentos obrantes en el mismo será el establecido en el presente* Real Decreto.

El Ministro de Defensa, o el órgano en quien este delegue, podrá acordar la exclusión de la consulta pública de aquellas series documentales o de aquellos documentos que, sin estar clasificados de acuerdo con la legislación de secretos oficiales, contengan información cuya difusión pueda afectar a la Defensa Nacional o a la Seguridad del Estado.

No obstante lo dispuesto en el párrafo anterior, cabrá solicitar autorización para el acceso a tales documentos o series documentales. Dicha autorización podrá ser concedida por el Ministro de Defensa, previo informe de la Comisión Calificadora de Documentos de la Defensa. La denegación de autorización deberá ser motivada.

Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos según establece la LPHE.

7.2.3. Documentos electrónicos clasificados

Según el art. 27 del Real Decreto 1708/2011, los documentos clasificados de conformidad con la normativa sobre secretos oficiales del Estado estarán excluidos de la consulta pública, sin que pueda concederse autorización para el acceso en tanto no recaiga una decisión de desclasificación por el órgano competente para realizarla.

Cuando la solicitud de consulta se refiera a documentos o series documentales que incorporen marcas de reserva o confidencialidad[15], el órgano competente para resolver remitirá la solicitud a su superior jerárquico o, en su caso al órgano que realizó la declaración de reserva o confidencialidad, para que decidan sobre la concesión de autorización de la consulta.

El procedimiento de clasificación de los documentos electrónicos se atendrá a lo establecido en Instrucción 64/2015.

[15] Las marcas de reserva o confidencialidad son las marcas de clasificación de los documentos oficialmente aceptadas que son 4: secreto, reservado, confidencial y difusión limitada.

El acceso a las series, expedientes y documentos electrónicos clasificados está fijado en los grupos de clasificación del Anexo IV de dicha Instrucción 64/2015 y en los procedimientos de reclasificación o desclasificación establecidos en la misma. Se entiende por desclasificación de la información el acto formal mediante el cual se anula de manera expresa la clasificación de la información. Este acto formal no será necesario si la autoridad u órgano que otorgó la clasificación señaló un plazo de duración de esta, o circunstancias que la condicionan.

Una vez desclasificados, los documentos quedarán sujetos al proceso de valoración y determinación del régimen de acceso en el archivo electrónico único del Ministerio de Defensa.

7.3. APLICACIÓN DE LAS CONDICIONES DE ACCESO

La aplicación de lo establecido en materia de acceso a los documentos electrónicos en los sistemas de información, tiene que poner en relación los objetos de acceso (documentos y sus agrupaciones) con los sujetos de acceso (agentes) y con las reglas que establecen los niveles de acceso (régimen de acceso).

En relación con los objetos de acceso (documentos y sus agrupaciones), las condiciones de acceso se aplican a la entidad documento y/o sus metadatos. La configuración del acceso a la documentación electrónica podrá realizarse, siempre que el análisis lo aconseje, en base a las series documentales de modo que los expedientes o agregaciones y documentos siempre hereden las condiciones de acceso y seguridad del nivel superior. Cuando las características de la documentación lo requieran, se podrán implementar condiciones de acceso diferenciadas para cada expediente individual, agregación individual, documento o partes del documento y metadatos de los mismos.

Los sujetos de acceso son los agentes que se relacionan con la entidad documento y pueden acceder a los sistemas de información en que se gestionan los documentos para crear, modificar, consultar y utilizar los objetos de acceso. Se establecerán los grupos de acceso en los entornos en que se gestionan los documentos de acuerdo a las directrices de seguridad del Ministerio de Defensa.

En relación al régimen de acceso determinado para los documentos electrónicos, se aplicará la seguridad adecuada, concretando los roles, permisos y controles asignados a los distintos agentes sobre los objetos de acceso.

Los requisitos de acceso y seguridad de los documentos deberán acompañar al análisis documental previo a la transformación digital de los procedimientos del Ministerio de Defensa.

Como resultado de dicho análisis documental, se elevarán a la Comisión Calificadora de Documentos de la Defensa las propuestas relativas al régimen de acceso. estas quedarán recogidas en un instrumento o tabla de acceso en soporte electrónico que permita, en cumplimiento al art. 26 del Real Decreto 1708/2011, poner a disposición del público la relación de documentos y series documentales de acceso restringido, con exclusión de aquellos que, en atención a los intereses protegidos, no deban ser objeto de publicidad.

El e-EMMDEF desarrollará los elementos de metadatos necesarios para el control y gestión del acceso y seguridad de los documentos electrónicos del Departamento a partir de los establecidos en el e-EMGDE 8 *Seguridad* y e-EMGDE 9 *Condiciones de acceso uso y reutilización*, y de las tablas de valores que se incluyen en el Anexo 6.

Cuando los documentos sean objeto de transparencia activa o reutilización, sus metadatos deben incluir información sobre los contenidos afectados y la referencia normativa correspondiente, especialmente a la LTAIP, siguiendo los criterios del elemento del e-EMGDE 9.2 *Condiciones de reutilización*.

Los documentos que estén sujetos a algún tipo de restricción de acceso deberán incluir metadatos relativos a las causas legales de dicha limitación siguiendo los criterios de codificación aplicables del e-EMGDE 9.1.1 *Código de la causa de limitación*.

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, siguiendo los criterios del elemento e-EMGDE 9.1.2. *Causa legal/normativa de limitación* y según la tabla de valores que se recoge en el anexo 6.

Cuando un documento contenga datos de carácter personal protegidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD) que no tengan la consideración de «fuentes accesibles al público» (tal y como se establece en el artículo 11 de la misma), deberá tener asignado un nivel de sensibilidad de datos de carácter personal siguiendo los criterios de la tabla de aplicación del elemento e-EMGDE 8.2 *Advertencia de seguridad*.

En los casos en que se deba proporcionar acceso parcial a un documento o a su contenido disociado de los datos restringidos, se podrá generar copia electrónica parcial auténtica bajo siguientes modalidades:

a) Enmascaramiento de datos: copia del documento en la que se han ocultado los datos susceptibles de protección.
b) Despersonalización o anonimización: copia del documento en la que se han ocultado los datos que identifican o permiten identificar fácilmente a las personas afectadas.
c) 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.
d) Limpieza de metadatos: borrado o modificación de los datos de autor, localización, aplicación o sistema de origen, etc.

El Ministerio de Defensa promoverá, en función de sus capacidades y recursos, la implantación progresiva de servicios telemáticos que permitan recoger, gestionar y dar respuesta a las solicitudes, reclamaciones y sugerencias que realicen los ciudadanos sobre acceso, localización, reproducción u otras cuestiones relacionadas con los documentos o los servicios que prestan los archivos del Sistema Archivístico de la Defensa.

La resolución del procedimiento que conceda el acceso expresará si es posible la obtención de copias y las condiciones de uso de las mismas. No se concederá en los siguientes supuestos:

a) Cuando los documentos no sean de libre consulta.
b) Cuando no resulte posible realizar la copia en un formato determinado debido a la carencia de equipos apropiados o al excesivo coste de la misma.

c) Cuando la reproducción suponga vulneración de los derechos de propiedad intelectual.

En relación con la generación de copias auténticas de los documentos electrónicos, su expedición estará sujeta a lo establecido en el art. 27 de la LPAC y a lo descrito en el anexo 1 de esta política.

8. Trazabilidad

La trazabilidad es la constancia de todas las acciones y procesos que se realizan sobre los documentos, los expedientes y los metadatos asociados a los mismos.

Como mínimo, los eventos que se registrarán sobre los documentos serán los siguientes:

a) La creación.
b) La modificación y versionado.
c) El borrado físico.
d) La transferencia a otro repositorio con cambio de custodia.
e) El acceso al contenido, cuando tenga un régimen de acceso que así lo requiera.

Para los expedientes y agregaciones documentales:

a) La creación.
b) La incorporación de nuevos elementos (documentos u otros expedientes).
c) La retirada de elementos (documentos u otros expedientes).
d) La creación y/o modificación del índice electrónico cuando corresponda.
e) El cierre sin posibilidad de agregar o eliminar más documentos.

f) La transferencia a otro almacenamiento con cambio de custodia.
g) La eliminación física.

La trazabilidad de las acciones deberá implementarse en los sistemas a través de los metadatos que establecen las relaciones de la entidad Actividad (que tipifica las acciones que se pueden realizar con los documentos) con las entidades Agente (que representan quién realiza las acciones) y Documento (sobre que objeto o nivel de agrupación se realizan).

El e-EMMDEF desarrollará los elementos de metadatos necesarios para el control de la trazabilidad de las acciones realizadas sobre los documentos electrónicos del Departamento a partir de los establecidos en el e-EMGDE 21 *Trazabilidad*.

e-EMGDE 21 – Trazabilidad.
- e-EMGDE 21.1 - Acción
  - 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.
- e-EMGDE 21.4 - Descripción.
- e-EMGDE 21.5 - Modificación de los metadatos.
- e-EMGDE 21.6 - Historia del cambio.
  - e-EMGDE 21.6.1 - Nombre del elemento.
  - e-EMGDE 21.6.2 - Valor anterior.

9. Identificación y período de validez de la PGDE-MINISDEF

Los datos identificativos principales son:

Nombre del documento	Política de gestión de documentos electrónicos en el Ministerio de Defensa
Versión	1.2
Identificador de la Política[16,17]	E00003301_1.2
URI de referencia de la Política	
Fecha de expedición	
Ámbito de aplicación	Documentos y expedientes producidos y/o custodiados por el Ministerio de Defensa.

9.1. 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

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

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

una política o versión posterior. En este caso, se podrá facilitar un período de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar los diferentes sistemas de gestión de documentos electrónicos utilizados por el Ministerio de Defensa a las especificaciones de la nueva versión.

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

Los anexos podrán ser actualizados sin necesidad de un proceso de revisión formal de la PGDE-MINISDEF. Asimismo, las referencias al esquema de metadatos e-EMGDE que se encuentran en el cuerpo principal serán actualizadas automáticamente sin necesidad de un proceso de revisión formal cuando se publiquen las sucesivas versiones.

9.2. IDENTIFICADOR DEL GESTOR DE LA POLÍTICA

Nombre del gestor	Subdirección General de Publicaciones y Patrimonio Cultural
Dirección de contacto	Paseo de Moret, 3 - 28008 Madrid
Identificador del gestor[18]	E04947701

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

10. Referencias

10.1. LEGISLACIÓN Y NORMATIVA

10.1.1. Ministerio de Defensa

i. Real Decreto 2598/1998, de 4 de diciembre, por el que se aprueba el Reglamento de Archivos Militares.
https://www.boe.es/buscar/pdf/1998/BOE-A-1998-29347-consolidado.pdf

ii. ORDEN DEF/315/2002, de 14 de febrero, por la que se aprueba el Plan Director de Sistemas de Información y Telecomunicaciones y se establece, para su dirección, gestión y seguimiento, el Comisionado del Plan
https://boe.es/boe/dias/2002/02/20/pdfs/A06752-06756.pdf

iii. ORDEN PRE/447/2003, de 27 de febrero, por la que se determinan los órganos de dirección, planificación y ejecución del Sistema Archivístico de la Defensa, se modifica la dependencia y composición de la Junta de Archivos Militares y se establece la dependencia y composición de la Comisión Calificadora de Documentos de la Defensa
https://www.boe.es/boe/dias/2003/03/04/pdfs/A08469-08472.pdf

iv. Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa.

v. Orden DEF/1766/2010, de 24 de junio, por la que se crea la Sede Electrónica Central del Ministerio de Defensa. http://www.boe.es/boe/dias/2010/07/02/pdfs/BOE-A-2010-10490.pdf

vi. Instrucción 41/2010, de 7 de julio, del Secretario de Estado de Defensa, por la que se aprueban las normas para la aplicación de la Política de Seguridad de la Información del Ministerio de Defensa.

vii. Resolución 4B0/38162/2010, de 8 de julio, del Instituto Social de las Fuerzas Armadas, por la que se crea y regula la Sede Electrónica del ISFAS. http://www.boe.es/boe/dias/2010/07/16/pdfs/BOE-A-2010-11348.pdf

viii. Instrucción 22/2016, de 11 de abril, del Secretario de Estado de Defensa, por la que se aprueban las normas para la Seguridad de la Información en las Personas.

ix. Instrucción 95/2011, de 16 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información en las Instalaciones.

x. Real Decreto 454/2012, de 5 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa https://www.boe.es/boe/dias/2012/03/06/pdfs/BOE-A-2012- 3162.pdf

xi. Instrucción 52/2013, de 17 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información del Ministerio de Defensa en poder de las empresas.

xii. Instrucción 51/2013, de 24 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información en los Documentos.

xiii. Real Decreto 872/2014, de 10 de octubre, por el que se establece la organización básica de las Fuerzas Armadas https://www.boe.es/boe/dias/2014/10/17/pdfs/BOE-A-2014-10520.pdf

xiv. Orden DEF/2594/2014, de 16 de diciembre, por la que se establece el sistema de utilización del código seguro de verificación de documentos electrónicos del Ministerio de Defensa.
http://www.boe.es/boe/dias/2015/01/26/pdfs/BOE-A-2015-632.pdf

xv. Orden DEF/1826/2015, de 3 de septiembre, por la que se regula el registro electrónico central del Ministerio de Defensa
https://boe.es/boe/dias/2015/09/09/pdfs/BOE-A-2015-9721.pdf

xvi. Real Decreto 837/2015, de 21 de septiembre, por el que se modifica el Real Decreto 454/2012, de 5 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa
https://www.boe.es/boe/dias/2015/09/22/pdfs/BOE-A-2015-10145.pdf

xvii. Orden DEF/2071/2015, de 5 de octubre, por la que se regula la Comisión Ministerial de Administración Digital del Ministerio de Defensa
https://www.boe.es/boe/dias/2015/10/09/pdfs/BOE-A-2015-10871.pdf

xviii. Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa
https://www.boe.es/boe/dias/2015/12/10/pdfs/BOE-A-2015-13385.pdf

xix. Instrucción 64/2015, de 7 de diciembre, del Secretario de Estado de Defensa, por la que se aprueban las Normas de seguridad de la información para la elaboración, clasificación, cesión, distribución y destrucción de información del Ministerio de Defensa.

10.1.2. Otras referencias

i. Ley 9/1968, de 5 de abril, sobre secretos oficiales
http://www.boe.es/buscar/pdf/1968/BOE-A-1968-444-consolidado.pdf

ii. Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales
https://www.boe.es/boe/dias/1969/02/24/pdfs/A02839-02842.pdf

iii. Ley 48/1978, de 7 de octubre por la que se modifica la Ley de 5 de abril de 1968, sobre Secretos Oficiales.
https://www.boe.es/boe/dias/1978/10/11/pdfs/A23605-23606.pdf

iv. Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
https://www.boe.es/boe/dias/1985/06/29/pdfs/A20342-20352.pdf

v. Acuerdo del Consejo de Ministros, de 28 de noviembre de 1986, por el que se clasifican determinados asuntos y materias con arreglo a la Ley de Secretos Oficiales, ampliado por Acuerdos del Consejo de Ministros de 17 de marzo y 29 de julio de 1994

vi. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
http://www.boe.es/buscar/pdf/1992/BOE-A-1992-26318-consolidado.pdf

vii. Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.
https://www.boe.es/buscar/pdf/1999/BOE-A-1999-11499-consolidado.pdf

viii. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
http://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

ix. Orden de 21 de diciembre de 2000 por la que se crea la Comisión calificadora de documentos administrativos del Ministerio del Interior y se regula el acceso a los archivos de él dependientes.
https://www.boe.es/buscar/pdf/2001/BOE-A-2001-334-consolidado.pdf

x. 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.
http://www.boe.es/boe/dias/2002/11/15/pdfs/A40139-40143.pdf

xi. Ley 59/2003, de 19 de diciembre, de firma electrónica.
http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

xii. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
https://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf

xiii. Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
https://www.boe.es/boe/dias/2007/11/17/pdfs/A47160-47165.pdf

xiv. 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.
http://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

xv. 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
https://www.boe.es/boe/dias/2009/11/18/pdfs/BOE-A-2009-18358.pdf

xvi. 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.
http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

xvii. 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.
http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf

xviii. 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.
http://www.boe.es/boe/dias/2011/11/25/pdfs/BOE-A-2011-18541.pdf

xix. Política de Firma Electrónica y de Certificados de la Administración General del Estado, aprobada por Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas.
http://www.boe.es/boe/dias/2012/12/13/pdfs/BOE-A-2012-15066.pdf

xx. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
http://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf

xxi. Orden INT/533/2014, de 19 de marzo, por la que se regulan las funciones, composición y funcionamiento de la Comisión Calificadora de Documentos Administrativos del Ministerio del Interior.
https://www.boe.es/boe/dias/2014/04/05/pdfs/BOE-A-2014-3653.pdf

xxii. Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos.
https://www.boe.es/boe/dias/2014/09/26/pdfs/BOE-A-2014-9741.pdf

xxiii. 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.
https://www.boe.es/boe/dias/2015/07/10/pdfs/BOE-A-2015-7731.pdf

xxiv. Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009, de 6 de noviembre, por el que se de-

sarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
https://www.boe.es/boe/dias/2015/07/18/pdfs/BOE-A-2015-8048.pdf

xxv. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
https://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10565.pdf

xxvi. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
https://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10566.pdf

10.2. NORMAS TÉCNICAS DE INTEROPERABILIDAD Y GUÍAS TÉCNICAS

i. 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.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13168.pdf

ii. 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.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13169.pdf

iii. Guía de aplicación de la Norma Técnica de Interoperabilidad de Documento Electrónico
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/BIBLIOTECA_PU_Publicacion_oficial_2011_documento_electronico_guia_de_aplicacion_NTI/Gu%C3%ADa%20de%20aplicaci%C3%B3n%20de%20la%20Norma%20T%C3%A9cnica%20de%20Interoperabilidad%20de%20Documento%20Electr%C3%B3nica.pdf

iv. 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.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13170.pdf

v. Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente Electrónico.
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/BIBLIOTECA_PU_Publicacion_oficial_2011_Expediente_electronico_guia_de_aplicacion_NTI/Gu%C3%ADa%20de%20aplicaci%C3%B3n%20de%20la%20Norma%20T%C3%A9cnica%20de%20Interoperabilidad%20de%20Expediente%20Electr%C3%B3nico.pdf

vi. 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.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011- 13171.pdf

vii. 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.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13172.pdf

viii. Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.
http://www.boe.es/boe/dias/2012/07/26/pdfs/BOE-A-2012-10048.pdf

ix. Guía de aplicación de la NTI de Política de Gestión de Documentos Electrónicos.
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/Guia_de_aplicacion_Politica_de_gestion_de_documento_electronico.pdf

x. Modelo de política de gestión de documentos electrónicos
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/NTI_Guia_de_aplicacion_Gestion_de_documento_electronico/20131128_Modelo_de_politica_de_gestion_de_documentos_electronicos_NIPO_630-13-166-8.pdf

xi. 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.
http://www.boe.es/boe/dias/2012/10/31/pdfs/BOE-A-2012-135

xii. Guía de aplicación de la Norma Técnica de Interoperabilidad de Catálogo de estándares
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/Guia_de_aplicacion_NTI_catalogo_de_estandares_Publicacion_oficial_2012/Guia_aplicacion_Norma_Tecnica_Interoperabilidad_Catalogo_de_estandares.pdf

10.3. DOCUMENTOS DE REFERENCIA

10.3.1. Ministerio de Defensa

i. Manual de digitalización para fondos bibliográficos, documentación de archivo y fondos museográficos.
http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=51506

ii. Manual de archivística
http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=71217

iii. Manual de organización de archivos de oficina
http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=71204

iv. Política de seguridad de la información del Ministerio de Defensa
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Tecnimap/pae_TECNIMAP_2006/

pae_TECNIMAP_2006_Comunicaciones_Presentadas_-_5/politica_de_seguridad_de_la_informacion.pdf

v. Procedimiento de uso de la firma electrónica longeva o de larga duración en los sistemas de información y telecomunicaciones del Ministerio de Defensa. PG-345-SEGINFO/01/13/V3

10.3.2. Estándares ISO

i. Norma UNE-ISO 15489-1:2006. Información y documentación. Gestión de documentos. Parte 1: Generalidades
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0035751

ii. Norma UNE-ISO 15489-2:2006. Información y documentación. Gestión de documentos. Parte 2: Directrices
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0037585

iii. Norma UNE-ISO 23081-1:2008. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 1: Principios
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0041438

iv. 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
http://isotc.iso.org/livelink/livelink/fetch/-8800112/8800136/8800147/N800R1_Construccion_de_un_esquema_de_metadatos_-_Por_Donde_Empezar_Metadatos_-_ESP.pdf?nodeid=11331471&vernum=-2

v. Norma UNE-ISO 30300:2011. Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0048671

vi. Norma UNE-ISO 30301:2011. Información y documentación. Sistemas de gestión para los documentos. Requisitos.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0048672

10.3.3. Otras referencias

i. MOD information policy (JSP 747). United Kingdom (Ministry of Defence). 2008
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/326158/JSP747_MOD_Information_Policy_V1.pdf

ii. Australian Government Recordkeeping Metadata Standard. 2008
http://www.naa.gov.au/Images/AGRkMS-Version-2.2-June-2015_tcm16-47131.pdf

iii. Guide to Recordkeeping in the Army - Army Publishing Directorate. 2008
http://www.apd.army.mil/pdffiles/p25_403.pdf

iv. Policy on the Retention and Disposition of NATO Information. 2009
http://www.nato.int/nato_static/assets/pdf/pdf_archives/20120327_C-M_2009_0021_INV-Retention_Dispo_of_NATO_Inf.pdf

v. Defence Records Management Policy Manual. Australian Government (Department of Defence). 2010
http://www.defence.gov.au/publications/manuals/polman3/polman3.pdf

vi. Australian Government Recordkeeping Metadata Standard Implementation Guidelines. 2011
http://www.naa.gov.au/records-management/publications/agrkms/implementation-guidelines.aspx

vii. NATO Records Policy. 2011
http://www.nato.int/nato_static/assets/pdf/pdf_archives/20120327_C-M_2011_0043-NRP.pdf

viii. Directive on the Management of Records Generated on operational deployment. NATO. 2012
http://www.nato.int/nato_static/assets/pdf/pdf_archives/20120327_C-M_2012_0014-Records_Operational_Deployment.pdf

ix. Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). 2012
http://administracionelectronica.gob.es/ctt/resources/Soluciones/381/Area%20descargas/Esquema-de-metadatos-para-la-Gestion-del-Documento-Electronico--e-EMGDE-.pdf?idIniciativa=381&idElemento=610

x. Defence records management policy and procedures (JSP 441). United Kingdom (Ministry of Defence). 2014
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/373694/20140402-JSP_441_Version_4_3_final_U.pdf

xi. Directive on the Preservation of NATO Digital Information of Permanent Value. 2014
http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_07/20141029_140703-AC_324-D_2014_0008.pdf

xii. Política de gestión de documentos electrónicos del Ministerio de Hacienda y Administraciones. 2014
http://www.minhap.gob.es/Documentacion/Publico/SGT/POLITICA%20DE%20GESTION%20DE%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20electronicos%20MINHAP.pdf

xiii. Guía de adecuación al Esquema Nacional de Interoperabilidad.2014
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/Normas_tecnicas/20141215_ENI_GuiaAdecuacion_ENI_PDF_NIPO_630-14-238-6/Guia_adecuacion_al_ENI_PDF_NIPO_630-14-238-6.pdf

xiv. Política de gestión de documentos electrónicos del Ayuntamiento de Cartagena. 2014
https://seguro.cartagena.es/sedeelectronica/docs/politica_gestion_documentos_electronicos.pdf

xv. Instruction: DoD Records Management Program. United States of America (Department of Defence). 2015
http://www.dtic.mil/whs/directives/corres/pdf/501502p.pdf

xvi. Política de Gestión de Documentos Electrónicos del Ministerio de Educación, Cultura y Deporte. 2015 http://www.mecd.gob.es/dms/mecd/cultura-mecd/areas-cultura/archivos/recursos-profesionales/documentos-electronicos/20150721-pgde-mecd-cuerpo/20150721-pgde-mecd-cuerpo.pdf

xvii. Anexos a la Política de Gestión de Documentos Electrónicos del Ministerio de Educación, Cultura y Deporte. 2015 http://www.mecd.gob.es/dms/mecd/cultura-mecd/areas-cultura/archivos/recursos-profesionales/documentos-electronicos/pgde-mecd-anexos-web/pgde-mecd-anexos-web.pdf

xviii. Política de gestión documental del Ayuntamiento de Barcelona. 2015 http://estatic.bcn.cat/ArxiuMunicipal/Continguts/Documents/Fitxers/Traduccions/InstruccioPoliticaGD_cast.pdf

xix. DECRETO 38/2016, de 5 de abril, del Gobierno de Aragón, por el que se aprueba la Política de gestión y archivo de documentos electrónicos de la Administración de la Comunidad Autónoma de Aragón y de sus Organismos Públicos http://www.boa.aragon.es/cgi-bin/EBOA/BRSCGI?CMD=VEROBJ&MLKOB=902540023535

xx. Normas de la Autoridad Nacional de Seguridad para la protección de la información clasificada. 2016 https://www.cni.es/comun/recursos/descargas/Normas_de_la_Autoridad_Nacional_para_la_Proteccion_de_la_Informacion_Clasificada.pdf

11. Glosario

11.1. TÉRMINOS

Acceso
Derecho, modo y medios de localizar, usar o recuperar la información y los documentos electrónicos que cumplen con los requerimientos establecidos en la política.

Activo
Cualquier bien que tiene valor para el Ministerio de Defensa.

Agente
Institución, sistema, persona física o jurídica responsable o involucrada en la creación, producción, custodia o gestión de documentos.

Agregación de documentos
Agrupación de documentos creada al margen de un procedimiento reglado.

Alta dirección
Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.

Ámbito
Campo de actividad. Competencia.

Los ámbitos del nivel específico del Ministerio de Defensa son:

a) Fuerzas Armadas
   1. Estado Mayor de la Defensa
   2. Ejército de Tierra
   3. Armada
   4. Ejército del Aire
b) Secretaría de Estado de Defensa
c) Subsecretaría de Defensa
d) Secretaría General de Política de Defensa.

Archivo

1) Conjunto orgánico de documentos producidos y/o recibidos en el ejercicio de sus funciones por las personas físicas o jurídicas, públicas y privadas.
2) La institución cultural donde se reúne, conserva, ordena y difunden los conjuntos orgánicos de documentos para la gestión administrativa, la información, la investigación y la cultura.
3) El archivo es también el local donde se conservan y consultan los conjuntos orgánicos de documentos.

Archivo electrónico único

Según la LPAC cada Administración Pública está obligada a mantener un archivo electrónico único de los documentos que correspondan a procedimientos finalizados, así como que estos expedientes sean conservados en un formato que permita garantizar la autenticidad, integridad y conservación del documento.

Auditoría

Proceso metodológico que consiste en la investigación de la eficacia de la gestión de los documentos electrónicos y el grado de cumplimiento de la normativa, con el objeto de proponer acciones de mejora o correctivas.

Autenticidad

Característica diplomática de los documentos que permite saber que un documento es lo que afirma ser, que ha sido creado/enviado por quien así lo afirma (y lo firma) y en el momento en que se afirma (se fecha).

Calendario de conservación
Cuadro que recoge todas las acciones dictaminadas en lo concerniente al tiempo de permanencia y las consiguientes acciones de disposición de las diferentes series documentales.

Calificación
Proceso documental que comprende la determinación de los documentos esenciales, la valoración de los documentos para determinación de los plazos de conservación y acciones de transferencia o eliminación y el dictamen de la autoridad calificadora.

Captura
Proceso de gestión de documentos en el que se produce la incorporación de estos en el sistema de gestión documental cumpliendo los requerimientos de la PGDE-MINISDEF, estableciéndose la relación fundamental que permanecerá inalterable entre el documento y su creador/receptor y el contexto en el que se creó/recibió por medio de los correspondientes metadatos.

Ciclo de vida de un documento electrónico
Conjunto de etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos, hasta su selección para conservación permanente o para su destrucción reglamentaria de acuerdo con la legislación.

Clasificación documental
Identificación y estructuración sistemática en categorías, de todos los documentos del Ministerio de Defensa de acuerdo a las funciones y actividades que los originan.

Comisión Calificadora de Documentos de la Defensa
Órgano específico del Ministerio de Defensa que estudia y dictamina las cuestiones relativas a la calificación y utilización de los documentos del Departamento, así como su integración en los archivos y el régimen de acceso e inutilidad administrativa de tales documentos.

Comisión Ministerial de Administración Digital del Ministerio de Defensa
Órgano colegiado responsable del impulso y de la coordinación interna del Departamento y sus organismos públicos adscritos en materia de Administración Digital y enlace con los órganos y comisiones relacionadas con las tecnologías de la información y las comunicaciones.

Confidencialidad
Característica que indica que solo pueden acceder a los documentos aquellos usuarios que tengan permiso reconocido o que sean destinatarios de los mismos.

Conservación
Procesos y operaciones realizados para garantizar las adecuadas condiciones de mantenimiento de los documentos a lo largo del tiempo.

Conversión
Proceso de transformación de los documentos de un formato a otro.

Copia auténtica
Nuevo documento, expedido por una organización con competencias atribuidas para ello, con valor probatorio pleno sobre los hechos o actos que documenta, equivalente al documento original.

Creación
Referido a un documento, momento en que se genera, y deberá realizarse preferiblemente en el momento más próximo a la actividad y por las personas que tengan asignada la competencia o función. No debe confundirse con la captura (véase captura).

Cuadro de clasificación
Estructura jerárquica y lógica, de carácter corporativo, que refleja las funciones y actividades del Ministerio de Defensa que dan lugar a la creación y recepción de documentos; sirve al objetivo de aportar el contexto de procedencia funcional de los documentos.

Custodia
Responsabilidad sobre los registros y archivos, su conservación adecuada y sobre todas las tareas derivadas de su gestión. No implica necesariamente la propiedad legal.

Custodio
Persona u organismo responsable de conservar adecuadamente y proteger un documento.

Desclasificación de la información
Acto formal mediante el cual se anula de manera expresa la clasificación de una información.

Descripción
Proceso que implica representar los documentos y sus niveles de agrupación mediante información estructurada en metadatos que servirán para su localización y su uso a lo largo de todo el ciclo de vida.

Destrucción de información
Proceso de eliminación y borrado de todos y cada uno de los elementos tangibles que le dan soporte, sin posibilidad de reconstrucción. Se considerará que no se ha destruido la información, si esta puede encontrarse en algún elemento tangible. El proceso de destrucción implicará que esta se elimine de todos los documentos o sistemas de información y telecomunicaciones en los que se encuentre.

Dictamen
Resultado del proceso de valoración documental en el que se manifiesta la decisión de la autoridad calificadora que establece los plazos de permanencia de los documentos en el sistema de gestión, las transferencias, el acceso y la eliminación o, en su caso, la conservación permanente.

Digitalización
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.

Disponibilidad
Característica del documento que indica que puede ser localizado, recuperado, presentado e interpretado en cualquier momento. Su presentación debería mostrar la actividad u operación que lo produjo.

Documentación
Conjunto de documentos que describen operaciones, decisiones, normas y procedimientos organizativos referidos a una determinada función, proceso o transacción.

Documento
Toda información creada, recibida y conservada como evidencia y como activo por el Ministerio de Defensa en el desarrollo de sus actividades o en virtud de sus obligaciones legales. Los documentos, en cualquier soporte, son la evidencia oficial de las acciones y decisiones del Departamento y forman parte de su patrimonio documental.

Documento electrónico
Según la LPAC, el documento electrónico es aquel que contiene información de cualquier naturaleza, archivada en un soporte electrónico, según un formato determinado, susceptible de identificación y tratamiento diferenciado. Dispone de los datos de identificación que permiten su individualización, sin perjuicio de su posible incorporación a un expediente electrónico; incorpora una referencia temporal del momento en que ha sido emitido y los metadatos mínimos exigidos, así como las firmas electrónicas que correspondan según lo previsto en la normativa aplicable.

Documento esencial o vital
Documento que resulta indispensable y vital para la continuidad digital del Ministerio de Defensa en caso de desastre o emergencia, permitiendo que pueda alcanzar sus objetivos, cumplir con sus obligaciones diarias de servicio y respetar la legalidad vigente y los derechos de las personas.

Documento simple
Unidad mínima de los niveles de agrupación documental.

Elaborador
Persona u organismo que materializa una información electrónica en forma de documento.

Esquema de metadatos
Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Expediente (en el ámbito de esta política)
Se considera expediente, dentro del ámbito de esta política, tanto a los expedientes administrativos como a cualquier otro tipo de expediente producido como consecuencia de un trámite y regulado por procedimientos particulares del ámbito de la defensa (operaciones militares, justicia, sanidad, etc.).

Expediente administrativo
Conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

Expurgo
Procedimiento que consiste en la identificación de los documentos que se van a destruir conforme a los plazos establecidos en la fase de valoración.

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

Fondo
Conjunto de documentos producidos o recibidos por un órgano o sujeto en el ejercicio de sus funciones o actividades y que aglutina un conjunto de series de la misma procedencia institucional.

Gestión de documentos
Conjunto de operaciones dirigidas al control de la creación, recepción, uso, valoración y conservación de los documentos.

Información de difusión limitada
Asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los grupos de secreto, reservado o confidencial, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

Información de uso oficial
Información cuya distribución esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo.

Información de uso público
Información cuya distribución NO esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo.

Información clasificada
Cualquier información o material respecto del cual se decida que requiere protección contra su divulgación o acceso no autorizados, por el daño o riesgo que esto supondría a los intereses del Estado, y al que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad.

Información confidencial
Asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los grupos de secreto o reservado, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar el cumplimiento de su misión.

Información no clasificada
Dependiendo de su ámbito de distribución, podrá ser información de uso oficial o de uso público.

Información pública
Contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de la LTAIP y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Información reservada
Asuntos, actos, documentos, informaciones, datos y objetos no comprendidos como información secreta por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a la Seguridad y Defensa del Estado.

Información secreta
Asuntos, actos, documentos, informaciones, datos y objetos que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello pudiera dar lugar a riesgos o perjuicios de la Seguridad y Defensa del Estado.

Integridad
Característica del documento que hace referencia a su carácter completo e inalterado.

Interoperabilidad
Capacidad de los sistemas de información, y por ende de los procedimientos a los que dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Materias clasificadas
Asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la Seguridad y Defensa del Estado. Se califican con las categorías de secreto y reservado en atención al grado de protección que requieran.

Metadatos
Se definen como « datos sobre los datos». En el contexto de la gestión de los documentos electrónicos, los metadatos son datos que describen el contexto, contenido y estructura de los documentos y su gestión a lo largo del tiempo.

Registro
Acto por el que se adjudica a un documento un identificador único en el momento de su entrada al sistema.

Responsabilidad
Principio por el que los individuos, las organizaciones y la sociedad asumen sus acciones y se les puede solicitar una explicación al respecto.

Seguridad de la información
Condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos establecidos para el correcto manejo y control de la información, en todo su ciclo de vida, así como para prevenir y detectar los posibles comprometimientos de la misma, que puedan afectar a su confidencialidad, integridad o disponibilidad.

Serie documental
Conjunto de unidades documentales de estructura y contenido homogéneos recibidas o producidas por un mismo órgano o sujeto productor en el ejercicio de cada una de sus funciones específicas.

Tesauro
Vocabulario controlado y especializado, formado por palabras utilizadas para indexar contenidos.

Transferencia
Procedimiento habitual de ingreso de fondos documentales en un archivo o repositorio, mediante el traslado de series o fracciones de serie una vez han cumplido el plazo de permanencia fijado en la valoración documental.

Trazabilidad
Constancia de todas las acciones y procesos que se realizan sobre los documentos, los expedientes y los metadatos asociados a los mismos.

Unidad
Agrupación de personal del Ministerio de Defensa con un papel definido, identidad, estructura y función concreta.

Usuario
Persona a la que el custodio de la información de un documento le permite el acceso a la misma.

Valoración documental
Proceso que comprende la investigación y el análisis de los testimonios administrativos, legales, jurídicos e informativos presentes en cada una de las series documentales. Como resultado se establecen las propuestas de los plazos de transferencia, la posible eliminación y el régimen de acceso a las mismas

11.2. ACRÓNIMOS

AA.PP: Administraciones Públicas.

AGE: Administración General del Estado.

ANS: Autoridad Nacional de Seguridad.

CCDD: Comisión Calificadora de Documentos de la Defensa.

CMAD: Comisión Ministerial de Administración Digital del Ministerio de Defensa.

CSCDA: Comisión Superior Calificadora de Documentos Administrativos.

CSV: Código Seguro de Verificación.

DIR3: Directorio Común de Unidades Orgánicas y Oficinas.

e-EMGDE: Esquema de Metadatos para la Gestión del Documento Electrónico.

e-EMMDEF: Esquema de Metadatos del Ministerio de Defensa.

ENI: Esquema Nacional de Interoperabilidad.

ENS: Esquema Nacional de Seguridad.

LOPD: Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

LPAC: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

LPHE: Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

LRISP: Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

LRJSP: Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

LSO: Ley 9/1968, de 5 de abril, sobre secretos oficiales.

LTAIP: Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

NATO: North Atlantic Treaty Organization (véase OTAN).

NS: Normas de la Autoridad Nacional de Seguridad para la protección de información clasificada.

NTI: Normas Técnicas de Interoperabilidad.

OTAN: Organización del Tratado del Atlántico Norte.

PGDE-MINISDEF: Política de gestión de documentos electrónicos del Ministerio de Defensa.

RAM: Reglamento de Archivos Militares.

SAD: Sistema Archivístico de la Defensa.

SEGINFODOC: Instrucción 51/2013, de 24 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas de Seguridad de la Información en los Documentos.

SGDE: sistema de gestión de documentos electrónicos.

SGDEA: sistema de gestión de documentos electrónicos de archivo.

SIA: Sistema de Información Administrativa.

SIR: Sistema de Interconexión de Registros.

TIC: Tecnologías de la Información y las Comunicaciones.

ANEXOS

ANEXO 1. Procedimiento instrumental para la expedición de copias electrónicas auténticas[1]

Una copia auténtica es un nuevo documento, expedido por una organización con competencias atribuidas para ello, con valor probatorio pleno sobre los hechos o actos que documenta, equivalente al documento original. En el momento de la expedición de una copia auténtica se acredita su autenticidad desde la perspectiva de su correspondencia con el original y tiene efectos certificantes en cuanto que garantiza la autenticidad de los datos contenidos. Según el artículo 27.2 de la ley 39/2015, las copias auténticas tendrán la misma validez y eficacia que los documentos originales. Para ello, serán realizadas mediante funcionario habilitado por la administración pública para la expedición de las mismas o mediante actuación administrativa automatizada.

Los efectos de las copias auténticas de documentos públicos (ya sean generados por la Administración o por el ciudadano) no se limitan al marco de un procedimiento administrativo determinado, sino que tienen la misma validez y eficacia que los documentos originales

[1] Tomado como referencia del apartado «2.3.Copiado auténtico de documentos» de la «Política de gestión del documento electrónico» del Ministerio de Educación, Cultura y Deporte, incluyendo la actualización legislativa incorporada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

produciendo idénticos efectos frente a las organizaciones y los interesados. En cambio, las copias auténticas de documentos privados surten únicamente efectos administrativos.

La copia auténtica puede consistir en la transcripción del contenido del documento original o en una copia realizada por cualquier medio informático, electrónico o telemático. Se expide a partir de:

a) El documento original.
b) Una copia auténtica.

Tal y como dicta el Real Decreto 1671/2009 en su artículo 43, la conservación de los originales es obligatoria.

Además, el artículo 51 del Real Decreto 1671/2009 dicta que en el caso de que el formato de los documentos y expedientes del archivo deje de figurar entre los admitidos en la gestión por el ENI, los responsables se encargarán del copiado auténtico con cambio de formato.

CARACTERÍSTICAS DE LA COPIA ELECTRÓNICA AUTÉNTICA

Según la ley 39/2015, en su artículo 27.2 t*endrán la consideración de copia auténtica de un documento público administrativo o privado las realizadas, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido*.

Para garantizar el carácter de copia auténtica, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, así como a las siguientes reglas:

a) Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.
b) Las copias electrónicas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización, requerirán que el documento haya sido digitalizado y deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

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

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

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

Por lo tanto, se admite la posibilidad de generar copias electrónicas auténticas a partir de otras copias electrónicas auténticas siempre que se observen los requisitos establecidos en los apartados anteriores.

CARACTERÍSTICAS DE LA COPIA ELECTRÓNICA AUTÉNTICA CON CAMBIO DE FORMATO

La copia electrónica con cambio de formato se obtiene a partir de la conversión, generando un nuevo documento electrónico con diferente formato o versión.

En el procedimiento de conversión se tendrá en cuenta:

a) La aplicación de los procedimientos de conversión descritos en la NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
b) La conservación del contenido, el contexto y la estructura del origen, así como la identificación de aquellos componentes que requieran tratamiento específico.
c) El nuevo formato debe:
    1.º Pertenecer al catálogo de estándares.
    2.º Permitir la reproducción de la información original sin pérdida de información.

Si se debe conformar como copia auténtica, se contemplarán los requisitos del apartado «Características de la copia electrónica auténtica».

En el metadato «Estado de elaboración» (e-EMGDE20) debe figurar el texto «EE02 (Copia electrónica auténtica con cambio de formato)».

COPIA ELECTRÓNICA PARCIAL AUTÉNTICA

La copia electrónica parcial auténtica se extrae del contenido de un único documento origen, permitiendo mantener la confidencialidad de los datos que no afecten al interesado.

En el metadato «Estado de elaboración» (e-EMGDE20) debe figurar «EE04 (Copia electrónica parcial auténtica)».

COPIA ELECTRÓNICA AUTÉNTICA DE DOCUMENTO ELECTRÓNICO PÚBLICO ADMINISTRATIVO

Según el artículo 27.4 de la ley 39/2015 indica que *los interesados podrán solicitar, en cualquier momento, la expedición de copias auténticas de los documentos públicos administrativos que hayan sido válidamente emitidos por las Administraciones Públicas. La solicitud se dirigirá al órgano que emitió el documento original, debiendo expedirse, salvo las excepciones derivadas de la aplicación de la Ley 19/2013, de 9 de diciembre, en el plazo de quince días a contar desde la recepción de la solicitud en el registro electrónico de la Administración u Organismo competente*.

La obtención de la copia podrá realizarse mediante extractos de los documentos o se podrá utilizar otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

La autenticidad de los documentos se verificará siguiendo las pautas de la NTI de Documento Electrónico.

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

El punto 6 de este mismo artículo refleja que *la expedición de copias auténticas de documentos públicos notariales, registrales y judiciales, así como de los diarios oficiales, se regirá por su legislación específica.*

COPIA ELECTRÓNICA AUTÉNTICA DE DOCUMENTOS EN SOPORTE NO ELECTRÓNICO

La misma ley 39/2015, en su artículo 27.4 regula que las *Administraciones Públicas estarán obligadas a expedir copias auténticas electrónicas de cualquier documento en papel que presenten los interesados y que se vaya a incorporar a un expediente administrativo.*

Define como «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.

Las imágenes electrónicas que realice la Administración se consideran copias electrónicas auténticas siempre que:

a) El documento que se copia sea original o copia auténtica.
b) En la copia electrónica estén incluidos los metadatos que acrediten su condición de copia y se visualicen al consultar el documento.
c) La imagen electrónica se codifique conforme a los formatos, niveles de calidad y condiciones técnicas especificadas en el ENI y se genere conforme a las normas establecidas.

En el metadato «e-EMGDE20 - Estado de elaboración» debe figurar «EE03 (Copia electrónica auténtica de documento papel)».

COPIA EN PAPEL AUTÉNTICA DE DOCUMENTOS ADMINISTRATIVOS ELECTRÓNICOS

El artículo 45 del Real Decreto 1671/2009 especifica los siguientes requisitos para que las copias emitidas en papel a partir de documentos electrónicos administrativos se consideren copias auténticas:

a) Que el documento electrónico sea:

   1.º Documento electrónico original.
   2.º Copia electrónica auténtica del documento electrónico original.
   3.º Copia electrónica auténtica del original en soporte papel.

b) Que incluya un código u otro sistema para la verificación de la copia mediante acceso a los archivos electrónicos del órgano u organismo público (Código Seguro de Verificación o CSV).
c) Que sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

DOCUMENTOS APORTADOS POR EL CIUDADANO

En el artículo 28, puntos 2 y 3 de la ley 39/2015, se especifica que los interesados no estarán obligados a aportar documentos elaborados por las administraciones públicas y que estas no exigirán al interesado la presentación de documentos originales, salvo excepciones.

Cuando excepcionalmente se solicite al interesado la presentación de un documento original y este estuviera en formato papel, el interesado deberá obtener una copia auténtica, cumpliendo con los requisitos del art. 27 de la ley 39/2015, con carácter previo a su presentación electrónica, Dicha copia electrónica deberá indicar expresamente esta circunstancia.

La ley 39/2015 omite el término «compulsa», que sí aparecía reflejado en normativa derogada por esta ley, dado que en su artículo 16, punto 5 indica que los documentos que se presenten presencialmente ante las administraciones públicas, deberán ser digitalizados, devolviéndose los originales al interesado, sin perjuicio de determinados supuestos en los que estos documentos deban ser custodiados por las mismas.

De la documentación presentada por el registro electrónico se emitirá automáticamente un recibo consistente en una copia autenticada del documento de que se trate, así como un recibo acreditativo de otros documentos que, en su caso, lo acompañen, que garantice la integridad y el no repudio de los mismos.

Dado que no se puede asegurar con plenas garantías la autenticidad de los documentos compulsados en origen, solo se admitirá la compulsa en destino, es decir, aquella realizada por el registro del organismo receptor de la documentación; o bien la compulsa realizada

por un fedatario público. En cualquier otro caso, se tratará el documento obtenido como «Copia».

En su punto 5 indica que de forma excepcional, *cuando la relevancia del documento en el procedimiento lo exija o existan dudas derivadas de la calidad de la copia, las Administraciones podrán solicitar de manera motivada el cotejo de las copias aportadas por el interesado, para lo que podrán requerir la exhibición del documento o de la información original*.

Las copias aportadas por el interesado tendrán eficacia exclusiva en el ámbito de la actividad de la Administración, siendo los interesados los responsables de la veracidad de los documentos que presenten.

DESTRUCCIÓN DE DOCUMENTOS EN SOPORTE NO ELECTRÓNICO

El artículo 46 del Real Decreto 1671/2009 establece que los documentos originales y las copias auténticas en papel o cualquier otro soporte no electrónico admitido por la ley como prueba, de los que se hayan generado copias electrónicas auténticas, se podrán eliminar en los siguientes casos:

a) Por resolución adoptada por el órgano responsable del procedimiento o custodia de los documentos, con dictamen previo de la Comisión Calificadora de Documentos de la Defensa y dictamen favorable de la Comisión Superior Calificadora de Documentos Administrativos cuando contemplen propuestas de exclusión o eliminación de bienes de patrimonio documental, según queda establecido en el art.13 y el Capítulo VI del RAM.
b) Si no se trata de documentos con valor histórico, artístico o de otro carácter relevante que aconseje su conservación y protección, o en el que figuren firmas u otras expresiones manuscritas o mecánicas que confieran al documento un valor especial.

El expediente de eliminación debe incluir un análisis de los riesgos relativos al supuesto de destrucción de que se trate, con mención explícita de las garantías de conservación de las copias electrónicas y del cumplimiento de las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establezca el ENS.

ANEXO 2. Control del cumplimiento del ENI en materia de gestión de documentos electrónicos[2]

RECUPERACIÓN Y CONSERVACIÓN DEL DOCUMENTO ELECTRÓNICO		
X.1	Se dispone de una Política de gestión de documentos electrónicos conforme a la *NTI de Política de Gestión de Documentos Electrónicos*.	1. No existe. 2. Se ha empezado a elaborar. 3. Existe un acuerdo informal consensuado sobre el contenido de la política. 4. Está elaborada pero pendiente de aprobar. 5. Está aprobada formalmente y publicada.
X.2	Se ha establecido un repositorio electrónico, complementario y equivalente en su función a los archivos convencionales gestionado en un sistema que contempla la aplicación de Normas de conservación a los documentos depositados en él y su transferencia a otros repositorios o archivos electrónicos.	1. No existe. 2. Se ha definido una norma o disposición para su creación. 3. Existe y se aplica de forma incipiente o progresiva. 4. Existe un Sistema de Gestión de Documentos Electrónicos (SGDE) que no contempla la conservación a largo plazo y se aplica plenamente a documentos administrativos

[2] Tomado del cuestionario para el seguimiento de la adecuación al ENI 2014 derivado de la «Guía de adecuación al Esquema Nacional de Interoperabilidad»

RECUPERACIÓN Y CONSERVACIÓN DEL DOCUMENTO ELECTRÓNICO		
		electrónicos y a cualquier otro documento susceptible de formar parte de un expediente-e. 5. Existe un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) que contempla la conservación a largo plazo y que se aplica plenamente y contempla normas de conservación y transferencia de los documentos entre repositorios.
X.3	Se han definido los calendarios de conservación de documentos electrónicos y de las series documentales.	1. <10% de las aplicaciones gestoras o alcanzado nivel 1 de madurez*. 2. 10%-40% de las aplicaciones gestoras o alcanzado nivel 2 de madurez*. 3. 40%-60% de las aplicaciones gestoras o alcanzado nivel 3 de madurez*. 4. 60%-90% de las aplicaciones gestoras o alcanzado nivel 4 de madurez*. 5. >90% de las aplicaciones gestoras o alcanzado nivel 5 de madurez*.
X.4	Se generan documentos electrónicos conforme a la NTI de Documento electrónico.	1. < 10% de los documentos o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los documentos o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los documentos o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los documentos o alcanzado nivel 4 de madurez*. 5. > 90% de los documentos o alcanzado nivel 5 de madurez*.
X.5	Se intercambian documentos electrónicos conforme al XSD publicado como Anexo a la NTI de Documento electrónico.	1. < 10% de los documentos o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los documentos o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los documentos o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los documentos o alcanzado nivel 4 de madurez*. 5. > 90% de los documentos o alcanzado nivel 5 de madurez*.

RECUPERACIÓN Y CONSERVACIÓN DEL DOCUMENTO ELECTRÓNICO		
X.6	Se generan expedientes electrónicos conforme a la NTI de Expediente electrónico.	1. < 10% de los expedientes o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los expedientes o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los expedientes o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los expedientes o alcanzado nivel 4 de madurez*. 5. > 90% de los expedientes o alcanzado nivel 5 de madurez*.
X.7	Se intercambian expedientes electrónicos conforme al XSD publicado como Anexo a la NTI de Expediente electrónico.	1. < 10% de los expedientes o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los expedientes o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los expedientes o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los expedientes o alcanzado nivel 4 de madurez*. 5. > 90% de los expedientes o alcanzado nivel 5 de madurez*.
X.8	Se ha definido en el organismo la normativa para la atribución de las competencias en cuanto a la generación de copias auténticas, tanto en lo referente a la producción en sentido estricto como a la autenticación de las copias.	0. No procede (n.a.) 1. No. 5. Sí.
X.9	Se generan copias auténticas, y en su caso se realizan conversiones, conforma a la NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.	1. < 10% de los casos o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los casos o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los casos o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los casos o alcanzado nivel4 de madurez*. 5. > 90% de los casos o alcanzado nivel 5 de madurez*.
X.10	Se aplica el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero) al repositorio electrónico.	1. < 10% de las medidas necesarias. 2. 10% - 40% de las medidas necesarias. 3. 40% - 60% de las medidas necesarias. 4. 60% - 90% de las medidas necesarias. 5. > 90% de las medidas necesarias.

RECUPERACIÓN Y CONSERVACIÓN DEL DOCUMENTO ELECTRÓNICO		
X.11	Los documentos y expedientes electrónicos se firman de acuerdo con la Política de firma electrónica y de certificados aplicable en el ámbito de la entidad.	1. < 10% de los documentos y expedientes o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los documentos y expedientes o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los documentos y expedientes o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los documentos y expedientes o alcanzado nivel 4 de madurez*. 5. > 90% de los documentos y expedientes o alcanzado nivel 5 de madurez*.
X.12	Se emplea la firma longeva para preservar la conservación de las firmas a lo largo del tiempo.	1. < 10% de los documentos firmados en que se considera necesario o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los documentos firmados en que se considera necesario o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los documentos firmados en que se considera necesario o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los documentos firmados en que se considera necesario o alcanzado nivel 4 de madurez*. 5. > 90% de los documentos firmados en que se considera necesario o alcanzado nivel 5 de madurez*.
X.13	La conservación de los documentos electrónicos atiende a lo previsto en los artículos 11 y 23 del RD 4/2010 y en la NTI de Catálogo de estándares.	1. < 10% de los documentos electrónicos o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los documentos electrónicos o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los documentos electrónicos o alcanzado nivel 3 de madurez*.

RECUPERACIÓN Y CONSERVACIÓN DEL DOCUMENTO ELECTRÓNICO		
		4. 60% - 90% de los documentos electrónicos o alcanzado nivel 4 de madurez*. 5. > 90% de los documentos electrónicos o alcanzado nivel 5 de madurez*.
X.14	Los documentos se digitalizan según lo previsto en la NTI de Digitalización de documentos.	0. No procede (n.a.) 1. < 10% de los casos o alcanzado nivel 1 de madurez*. 2. 10% - 40% de los casos o alcanzado nivel 2 de madurez*. 3. 40% - 60% de los casos o alcanzado nivel 3 de madurez*. 4. 60% - 90% de los casos o alcanzado nivel 4 de madurez*. 5. > 90% de los casos o alcanzado nivel 5 de madurez*.
X.15	Se incorporan expedientes y documentos electrónicos a los repositorios electrónicos	1. < 10% de los documentos y expedientes electrónicos. 2. 10% - 40% de los documentos y expedientes electrónicos. 3. 40% - 60% de los documentos y expedientes electrónicos. 4. 60% - 90% de los documentos y expedientes electrónicos. 5. > 90% de los documentos y expedientes electrónicos.
X.16	Indique cuáles son los medios tecnológicos utilizados para los repositorios electrónicos (p.e. software de gestión documental, etc.)	[Texto libre]

ANEXO 3. Consideraciones para el desarrollo del esquema de metadatos del Ministerio de Defensa

ESQUEMA DE METADATOS Y PERFILES DE APLICACIÓN

El documento ISO/TC 46/SC 11 N800R1, «Orientaciones sobre la elaboración de un esquema de metadatos» Figura 1, diferencia entre:

a) Esquema de metadatos: plan lógico que muestra las relaciones entre los distintos elementos del conjunto de metadatos, normalmente mediante el establecimiento de reglas para su uso y gestión y específicamente relacionados con la semántica, la sintaxis y la obligatoriedad de los valores.
b) Perfil de aplicación: define el uso de los elementos de metadatos incluidos en un conjunto de elementos. Mientras que un conjunto de elementos establece conceptos, expresados por los propios elementos de metadatos, y se enfoca sobre la semántica o los significados de aquellos elementos, un perfil de aplicación va más lejos y añade las reglas de la organización y las directrices en el uso de los elementos. Identifica las obligaciones y limitaciones de los elementos, y proporciona comentarios y ejemplos para ayudar a la compresión de los elementos. Los perfiles de aplicación pueden incluir elementos integrados procedentes de uno o más conjuntos de elementos permitiendo de este modo a una aplicación determinada cumplir sus requisitos funcionales.

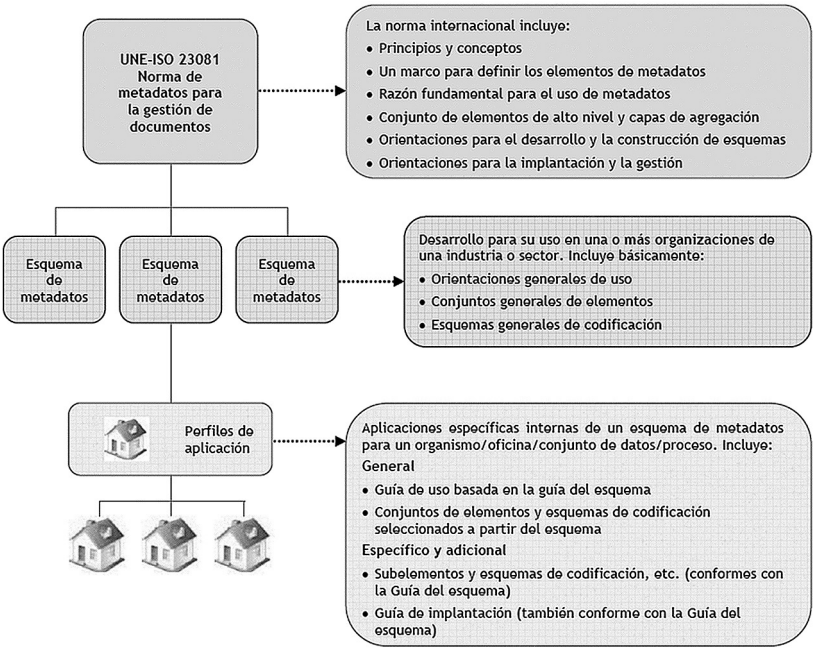

Figura 1.

El Ministerio de Hacienda y Administraciones Públicas ha desarrollado como documentación complementaria a la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos, el Esquema de Metadatos para la Gestión del Documento Electrónico **e-EMGDE.** Este se basa en el propuesto y utilizado por el Archivo Nacional de Australia *Australian Government Recordkeeping Metadata Standard Version 2.0*, y tiene en cuenta los requisitos de las restantes Normas Técnicas de Interoperabilidad y la legislación vigente.

Las administraciones que utilicen dicho esquema de metadatos deben implementar los elementos y sub-elementos obligatorios en las condiciones de uso e implantación contenidas en dicho documento. Los organismos de la Administración del Estado, como práctica común, están adoptando este esquema y desarrollando sus perfiles específicos de aplicación. Otros ámbitos con autonomía regulatoria en

materia de gestión documental y archivos optan por desarrollar sus propios esquemas tomando como referencia el e-EMGDE o el estándar australiano de origen.

En el Ministerio de Defensa se combina el hecho de ser organismo de la AGE y de disponer de un sistema archivístico propio. De igual modo, y en lo que concierne a la interoperabilidad, el Departamento está obligado a ser interoperable con los organismos de la administración española y con los organismos internacionales de la defensa de los que es miembro. Ello, unido a las dimensiones y complejidad del Departamento hace aconsejable el desarrollo de un esquema de metadatos propio que, basado en el e-EMGDE, contemple los posibles elementos específicos del Sistema Archivístico de la Defensa y requisitos de interoperabilidad internacionales. Dicho esquema ha sido denominado en la política de gestión de documentos e-EMMDEF y requerirá además de uno o varios perfiles de aplicación según lo aconsejen los sistemas empleados en la gestión de los documentos electrónicos o las necesidades específicas de los organismos ministeriales.

Los metadatos para la gestión de documentos se pueden obtener de múltiples fuentes. Algunos metadatos pueden existir ya y ser utilizados para otros fines dentro de los sistemas de gestión de información del Ministerio de Defensa. Muchas de las propiedades de los metadatos se pueden asignar automáticamente en el proceso de creación y captura de los documentos, mientras que otros pueden ser atribuidos en diferentes momentos durante la vida útil del documento. Esta idea de que los metadatos pueden ser acumulativos, permite ser flexibles en cuanto al tipo y la cantidad de metadatos que se aplican a los documentos en diferentes etapas de su vida: por ejemplo, existirán expedientes y documentos que puedan ser clasificados desde el origen y habrá casos en los que el proceso de clasificación se realice en la transferencia al sistema de conservación a largo plazo. La elaboración del e-EMMDEF, y su perfil o perfiles, requerirá un estudio en profundidad de la situación de partida y de las necesidades y requisitos que afectan a la documentación del Departamento. Además, será necesario identificar y documentar, a nivel de sistemas, los esquemas descriptivos que se vayan a utilizar como fuente de valores de datos para determinadas propiedades de metadatos de los documentos.

MODELO DE IMPLEMENTACIÓN

En el punto 3.3 de la PGDE-MINISDEF se plantea la adopción de un enfoque de implementación de metadatos multientidad tal como recomiendan las mejores prácticas internacionales.

Los beneficios del modelo multientidad son:

a) Una aplicabilidad más amplia para su empleo en múltiples sistemas del Departamento, no solo en las aplicaciones de gestión documental.
b) Mayor potencial de reutilización de la información descriptiva estructurada que ya pueda existir dentro de los distintos sistemas de la organización.
c) Disponibilidad de una información contextual más rica a la hora de facilitar la comprensión de las acciones y decisiones tomadas sobre la misma (históricos de cambios en la información y en sus relaciones).

Los documentos de referencia a seguir para abordar la implementación son: el *Ejemplo de aplicación del Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE)* publicado por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica y disponible en el Portal de Administración Electrónica (PAe): https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/Normas_tecnicas/20130517_ENI_Ejemplo_eEMGDE_2/2013_Ejemplo_de_eEMGDE_NIPO_630-13-181-4.pdf

y el *«Australian Government Recordkeeping Metadata Standard Implementation Guidelines» v.2.2., 2015*, que es base del e-EMGDE como ya se ha indicado y está disponible en http://www.naa.gov.au/records-management/publications/agrkms/implementation-guidelines.aspx

Este último, elaborado a partir de la experiencia de más de 15 años en la aplicación de un esquema de metadatos estandarizado, establece recomendaciones muy detalladas para la implementación: desde un modelo monoentidad (documento) a un modelo parcial - dos entidades (documento y agente) tres entidades (documento, agente, actividad o documento agente, relación) hasta una implementación completa de las cinco entidades (documento, agente, actividad, regulación y relación).

Uno de los componentes centrales del enfoque multientidad es el uso de la entidad relación para describir los eventos que afectan a los documentos. La entidad relación:

a) Une dos o más instancias de entidades relacionadas (por ejemplo, una serie de expediente identificada como «A3525», y la propiedad de una organización llamada «IP INTA», con una organización llamada «Instituto nacional de Técnica Aeroespacial»).
b) Proporciona información sobre el evento o acción en la que se vincularon esas instancias de la entidad (en el ejemplo anterior, «posee» y/o «transfiere»).

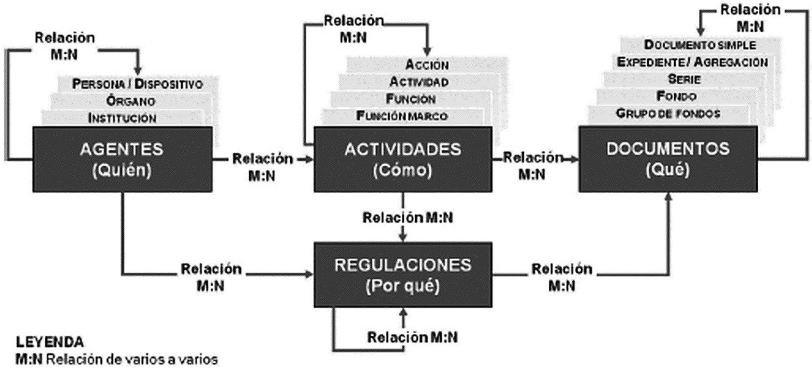

Figura 2: Modelo multientidad de metadatos para la gestión de los documentos. E-EMGDE.

Mediante el uso de las propiedades: tipos de relación, nombres de relación predefinidos y el intervalo de fechas, descripción, entidad relacionada e historial de cambios, la entidad relación puede registrar información acerca de los eventos a medida que ocurren.

Los metadatos de la entidad relación, al igual que el resto de los metadatos de los documentos, deben estar relacionados con los documentos de forma persistente. Esto significa que deben ser conservados en los sistemas (no sobreescritos), y permanecer ligados, o almacenados con los documentos. Los eventos (relaciones) que se producen, a menudo cambian los valores actuales de las propiedades particulares de determinados metadatos, por lo que en determinados casos se debe mantener el

histórico separado de los acontecimientos que han tenido lugar (ejemplo una transferencia, un cambio de repositorio) y de los cambios en los valores de los metadatos resultantes de los mismos. Estos históricos de cambios pueden ser mantenidos con propósito general (no solo para los documentos electrónicos) para otros fines del Departamento como sería por ejemplo el registro de cambios y actualizaciones normativas a través del uso de la entidad regulación (ej. política de firma) o los cambios en la estructura orgánica y titulares a través del uso de la entidad agente.

Dada la dimensión y complejidad del Ministerio de Defensa, puede optarse por avanzar con un enfoque estratégico hacia una implementación multientidad, e ir aplicando modelos parciales o incluso de tipo monoentidad en aquellos organismos, unidades o sistemas que así lo aconsejen.

Las características técnicas de la implementación de los metadatos deberán definirse en el programa de tratamiento de los documentos previsto en el punto 2.7 de la PGDE-MINISDEF.

TABLA DE METADATOS DE REFERENCIA PARA EL E-EEMDEF

Un esquema de metadatos incluye propiedades de metadatos obligatorios, condicionales y opcionales y sub-propiedades que se utilizan en la descripción de las entidades. En implementaciones multientidad, las propiedades obligatorias deben aplicarse a todas las entidades competentes para garantizar que las descripciones sean completas, exactas, fiables y utilizables. El uso de propiedades condicionales depende de otros factores o circunstancias. Las propiedades opcionales mejoran las descripciones de entidades, pero su uso y retención pueden no ser de aplicación a todas las necesidades del Departamento.

La estructura de metadatos con indicación de la obligatoriedad y aplicabilidad que figura en la tabla resumen que se muestra a continuación, responde al modelo conceptual entidad-relación del Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE)[3]

[3] http://administracionelectronica.gob.es/ctt/resources/Soluciones/381/Area%20descargas/Esquema-de-metadatos-para-la-Gestion-del-Documento-Electronico--e-EMGDE-.pdf?idIniciativa=381&idElemento=610

y del perfil de aplicación del Ministerio de Deporte Educación y Cultura, y que puede servir de base para el futuro desarrollo del esquema del Ministerio de Defensa.

ELEMENTO	OBLIGATORIO			APLICABILIDAD				
	Obligatorio	Condicional	Opcional	Documento	Agente	Actividad	Regulación	Relación
0 - TIPO DE ENTIDAD		√		√	√	√	√	√
1 - CATEGORÍA	√			√	√	√	√	√
2 - IDENTIFICADOR	√			√	√	√	√	√
2.1 – Secuencia de identificador	√			√	√	√	√	√
2.2 – Esquema de identificador		√		√	√	√	√	√
3 – NOMBRE		√		√	√	√	√	√
3.1 – Nombre natural		√		√	√	√	√	√
3.2 – Esquema de nombre		√		√	√	√	√	√
4 – FECHAS	√			√	√	√	√	√
4.1 – Fecha inicio	√			√	√	√	√	√
4.2 – Fecha fin		√		√	√	√	√	√
5 – DESCRIPCIÓN			√	√	√	√	√	√
6 – ENTIDAD RELACIONADA	√			x	x	x	x	√
6.1 – ID de entidad relacionada	√			x	x	x	x	√
6.2 – Esquema de ID de entidad relacionada		√		x	x	x	x	√
6.3 – Rol de la relación	√			x	x	x	x	√
7 – JURISDICCIÓN			√	√	√	√	√	x
8 - SEGURIDAD		√		√	x	√	√	x
8.1 – Clasificación de seguridad		√		√	x	√	√	x
8.1.1 – Clasificación de acceso		√		√	x	√	√	x
8.1.2 – Código de la Política de control de acceso		√		√	x	√	√	x
8.2 – Advertencia de seguridad		√		√	x	√	√	x

ELEMENTO	OBLIGATORIO			APLICABILIDAD				
	Obligatorio	Condicional	Opcional	Documento	Agente	Actividad	Regulación	Relación
8.2.1 – Texto de la advertencia		√		√	x	√	√	x
8.2.2 – Categoría de la advertencia		√		√	x	√	√	x
8.3 – Permisos		√		x	√	√	x	x
8.4 – Sensibilidad datos de carácter personal		√		√	x	√	√	x
8.5 – Clasificación ENS		√		√	√	√	√	x
8.6 – Nivel de clasificación de la información		√		√	x	x	x	x
9 – DERECHOS DE ACCESO, USO Y REUTILIZACIÓN		√		√	x	x	x	x
9.1 – Tipo de acceso		√		√	x	x	x	x
9.1.1 – Código de la causa de limitación		√		√	x	x	x	x
9.1.2 – Causa legal/normativa de limitación		√		√	x	x	x	x
9.2 – Condiciones de reutilización		√		√	x	x	x	x
10 – CONTACTO		√		x	√	x	x	x
10.1 – Tipo de contacto		√		x	√	x	x	x
10.2 – Dato de contacto		√		x	√	x	x	x
10.3 – Puesto		√		x	√	x	x	x
11 – IDIOMA		√		√	√	x	x	x
12 – PUNTOS DE ACCESO			√	√	x	x	√	x
12.1 – Término punto de acceso			√	√	x	x	√	x
12.2 – ID de punto de acceso			√	√	x	x	√	x
12.3 – Esquema		√		√	x	x	√	x
13 – CALIFICACIÓN		√		√	x	x	x	x
13.1 – Valoración		√		√	x	x	x	x
13.1.1 – Valor primario		√		√	x	x	x	x
13.1.1.1 – Tipo de valor		√		√	x	x	x	x

ELEMENTO	OBLIGATORIO			APLICABILIDAD				
	Obligatorio	Condicional	Opcional	Documento	Agente	Actividad	Regulación	Relación
13.1.1.2 – Plazo		√		√	x	x	x	x
13.1.2 – Valor secundario		√		√	x	x	x	x
13.2 – Dictamen		√		√	x	x	x	x
13.2.1 – Tipo de dictamen		√		√	x	x	x	x
13.2.2 – Acción dictaminada		√		√	x	x	x	x
13.2.3 – Plazo de ejecución de acción dictaminada		√		√	x	x	x	x
13.3 – Transferencia		√		√	x	x	x	x
13.1.1 – Fase de archivo		√		√	x	x	x	x
13.3.2 – Plazo de transferencia		√		√	x	x	x	x
13.4 – Documento esencial		√		√	x	x	x	x
14 – CARACTERÍSTICAS TÉCNICAS	√			√	x	x	x	x
14.1 – Formato	√			√	x	x	x	x
14.1.1 – Nombre del formato	√			√	x	x	x	x
14.1.2 – Extensión del fichero	√			√	x	x	x	x
14.2 – Versión de formato			√	√	x	x	x	x
14.3 – Resolución			√	√	x	x	x	x
14.4 – Tamaño		√		√	x	x	x	x
14.4.1 – Dimensiones físicas		√		√	x	x	x	x
14.4.2 – Tamaño lógico			√	√	x	x	x	x
14.4.3 – Cantidad			√	√	x	x	x	x
14.4.4 – Unidades		√		√	x	x	x	x
14.5 – Profundidad de color			√	√	x	x	x	x
15 – UBICACIÓN			√	√	x	x	x	x
15.1 – Soporte		√		√	x	x	x	x
15.2 – Localización			√	√	x	x	x	x

ELEMENTO	OBLIGATORIO			APLICABILIDAD				
	Obligatorio	Condicional	Opcional	Documento	Agente	Actividad	Regulación	Relación
16 – VERIFICACIÓN DE INTEGRIDAD		√		√	x	x	x	x
16.1 - Algoritmo		√		√	x	x	x	x
16.2 – Valor		√		√	x	x	x	x
17 – FIRMA	√			√	x	x	x	x
17.1 – Tipo de firma	√			√	x	x	x	x
17.2 – Valor del CSV		√		√	x	x	x	x
17.3 – Definición generación CSV	√			√	x	x	x	x
17.4 – Firmante			√	√	x	x	x	x
17.4.1 – Nombre y apellidos o razón social			√	√	x	x	x	x
17.4.2 – Número de identificación de los firmantes			√	√	x	x	x	x
17.4.3 – En calidad de			√	√	x	x	x	x
17.4.4 – Nivel de firma			√	√	x	x	x	x
17.4.5 – Información adicional			√	√	x	x	x	x
18 – TIPO DOCUMENTAL	√			√	x	x	x	x
19 – PRIORIDAD			√	√	x	√	x	x
20 – ESTADO DE ELABORACIÓN	√			√	x	x	x	x
21 – TRAZABILIDAD[4]		√		√	√	√	√	√
21.1 – Acción		√		√	√	√	√	√
21.1.1 – Fecha de la acción		√		√	√	√	√	√
21.1.2 – Entidad de la acción		√		√	√	√	√	√
21.2 – Motivo reglado		√		√	√	√	√	√
21.3 – Usuario de la acción		√		√	√	√	√	√

[4] Tomado de e-EMGDE versión 052012, más la adición de 21.1.1 y 21.1.2, de la versión 20112014.

ELEMENTO	OBLIGATORIO			APLICABILIDAD				
	Obligatorio	Condicional	Opcional	Documento	Agente	Actividad	Regulación	Relación
21.4 – Descripción			√	√	√	√	√	√
21.5 – Modificación de los metadatos		√		√	√	√	√	√
21.6 – Historia del cambio		√		x	x	x	x	√
21.6.1 – Nombre del elemento		√		x	x	x	x	√
21.6.2 – Valor anterior		√		x	x	x	x	√
22 – CLASIFICACIÓN[5]	√			√	√	√	√	√
22.1 – Código de clasificación[5]	√			√	√	√	√	√
22.2 – Denominación de clase[5]	√			√	√	√	√	√
22.3 – Tipo de clasificación (SIA/ funcional)[5]	√			√	√	√	√	√
23 – VERSIÓN NTI[5]	√			√	x	x	x	x
24 – ÓRGANO[5]	√			√	x	x	x	x
25 – ORIGEN DEL DOCUMENTO[5]	√			√	x	x	x	x
26 – IDENTIFICACIÓN DEL DOCUMENTO ORIGEN[5]		√		√	x	x	x	x
27 – ESTADO DEL EXPEDIENTE[5]	√			√	x	x	x	x
28 – INTERESADO[5]	√			√	x	x	x	x
29 – ASIENTO REGISTRAL[5]			√	√	x	x	x	x
29.1 – Tipo de asiento registral[5]			√	√	x	x	x	x
29.2 – Código de la oficina de registro[5]			√	√	x	x	x	x
29.3 – Fecha del asiento registral[5]			√	√	x	x	x	x
29.4 – Número de asiento registral[5]			√	√	x	x	x	x

[5] Tomado de e-EMGDE versión 20112014.

ANEXO 4. Esquema funcional para el desarrollo del cuadro de clasificación documental de los documentos electrónicos[6]

Partiendo del análisis documental, se desarrollará un cuadro de clasificación funcional en los 4 niveles establecidos en el e-EMGDE para el esquema de categorías de la entidad Actividad; a modo de ejemplo:

N1 FUNCIÓN MARCO: **Administración y gestión**
N2 FUNCIÓN: **Contratación**
N3 ACTIVIDAD: **Contratación de bienes y servicios**
N4 ACCIÓN: **Contratación de suministros, equipos militares, armas y municiones**

Mediante la relación de las entidades de metadatos se deberá componer el cuadro de clasificación orgánico funcional a aplicar a los documentos: la serie documental (entidad documento) estará relacionada con el nivel más específico de clasificación funcional (entidad

[6] Esquema basado en el Real Decreto 454/2012, de 5 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, y su modificación mediante RD 524/2014. También se han estudiado como referencia los cuadros de clasificación, del Ministerio de Defensa Australiano y Ministerio de Defensa del Reino Unido, y del Ministerio de Defensa para la Armada de Estados Unidos.

actividad), y con la unidad productora (entidad agente). A modo de ejemplo:

Serie documental = Expedientes de contratación de suministros de equipos militares.
Actividad =Contratación de suministros, equipos militares, armas y municiones.
Agente = Ejército de Tierra.

Se enuncia de manera no exhaustiva el esquema funcional provisional para el primer y segundo nivel de clasificación documental:

DIRECCIÓN Y ESTRATEGIA

Política de defensa (Preparación-planeamiento, desarrollo y ejecución)
Política económica (preparación, dirección y desarrollo)
Política de armamento y material (preparación, dirección y desarrollo)
Política de infraestructuras (preparación, dirección y desarrollo)
Política industrial de la defensa
Cultura de seguridad y defensa
Comunicación, relaciones informativas y publicidad institucional
Representación militar en el exterior y relaciones internacionales
Estrategia militar (definición y desarrollo)
Inteligencia militar
Investigación, desarrollo e innovación
Emergencias y situaciones de crisis
Normativa: órdenes, procedimientos e instrucciones

ADMINISTRACIÓN Y GESTIÓN

Gestión y control de los recursos humanos
Gestión y control de los recursos materiales
Gestión y control de los recursos financieros
Contratación
Desarrollo organizativo
Coordinación territorial
Gestión de las infraestructuras
Gestión medioambiental y energética

Proyectos y obras
Gestión de bienes muebles
Gestión de bienes inmuebles
Gestión de los sistemas y tecnologías de información y comunicaciones y de seguridad de la información
Gestión de bibliotecas, museos, archivos y patrimonio cultural
Comercio exterior de material, de productos y tecnologías de la defensa
Gestión del armamento y material
Gestión de la actividad industrial de la defensa
Planificación y gestión de proyectos
Procedimiento administrativo y recursos contencioso-administrativos
Gestión de publicaciones
Gestión de la información y atención al ciudadano
Asesoría jurídica
Intervención

OPERACIONES DE LAS FUERZAS ARMADAS

Planificación de operaciones
Conducción de operaciones
Seguimiento de operaciones
Operaciones de mantenimiento de la paz

PREPARACIÓN DE LAS FUERZAS ARMADAS

Definición y evaluación de capacidades
Reclutamiento y enseñanza militar
Adiestramiento, preparación y evaluación de las unidades
Mantenimiento de la fuerza y apoyo logístico
Sistemas de armas y apoyo

ACTIVIDADES ESPECÍFICAS

Acción social
Aeronavegabilidad
Cartografía e Hidrografía
Cría caballar
Estudios de la Defensa

Hidrodinámica
Ingeniería
Jurisdicción militar
Obras
Penitenciaría militar
Policía Militar
Reservistas voluntarios
Residencias militares
Sanidad militar
Técnica aeroespacial
Vivienda

ANEXO 5. Medidas para la preservación a largo plazo

CONSERVACIÓN DE LOS DOCUMENTOS ELECTRÓNICOS

La norma UNE *ISO/TR 18492:2008 «Conservación a largo plazo de información electrónica basada en documentos»* define conservación a largo plazo como «el periodo de tiempo en el que la información electrónica se mantiene como evidencia accesible y auténtica» y aclara que este periodo puede abarcar desde unos pocos años a cientos de años dependiendo de las necesidades y requisitos de las organizaciones.

El proceso de conservación –sinónimo en este documento de preservación– debe aplicarse de manera continua a lo largo de todo el ciclo de vida de los documentos electrónicos para asegurar su recuperación, tal como señala el Esquema Nacional de Interoperabilidad en su artículo 21.

Obviamente no puede contemplarse de forma aislada de otros procesos de gestión documental. De hecho, existen algunos requisitos, derivados de estos mismos procesos, que facilitarán su desarrollo e implementación, como son:

a) Disponer de un cuadro de clasificación basado en las funciones del organismo. Este es un requisito crucial para abordar el proceso de conservación, ya que permite la organización de

los documentos y expedientes electrónicos y, especialmente, la determinación de qué datos (o documentos) serán objeto de un tratamiento diferenciado para ser conservados.

b) Calificación del valor de las series documentales, que ayudará a ubicar los documentos electrónicos en los soportes de almacenamiento más adecuados, tanto en relación a su coste como a sus características de rendimiento.

c) Asociado al cuadro de clasificación, es indispensable contar con un calendario de conservación, definido en el RD 1708/2011, de 18 de noviembre, por el que se establece el sistema Español de Archivos, como «el instrumento de trabajo fruto del proceso de valoración documental, en el que se recoge el plazo de permanencia de los documentos de archivo en cada una de las fases del ciclo vital para su selección, eliminación o conservación permanente y, en su caso, el método y procedimiento de selección, eliminación o conservación en otro soporte».

Asimismo, para determinar el entorno concreto y el alcance de este proceso, sería recomendable identificar los sistemas de información que manejan documentos electrónicos y los sistemas de almacenamiento, soportes y tecnologías involucrados.

Por último, con el objetivo de cumplir adecuadamente los preceptos del Esquema Nacional de Interoperabilidad, las administraciones públicas deben contar con un plan de preservación de los documentos electrónicos que deben conservarse a largo plazo. Esto es especialmente importante para el Ministerio de Defensa que asume plenas competencias en materia de archivo histórico.

El plan de preservación digital definirá:

a) Los actores implicados en el proceso de conservación del documento electrónico.

b) Los elementos a proteger (activos), detallando sus características, las interdependencias entre ellos y las medidas de protección ya adoptadas o disponibles.

c) 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.

d) La estrategia de preservación a adoptar.
e) Las medidas de prevención que se adopten para cada tipo o grupo de riesgos.

El objetivo del plan será garantizar la accesibilidad, autenticidad, disponibilidad, integridad, trazabilidad, inteligibilidad y legibilidad de los documentos electrónicos a lo largo de su ciclo de vida, frente a los cinco grupos de riesgos que se desarrollan en el **punto 3** de este anexo.

Para el desarrollo del plan de preservación, se tomarán como referencia la estrategia y directrices de la OTAN: AC/324-D(2012)0003, NATO Strategy for the Long Term Preservation of Digital Information y AC/324- D(2014)0008 Directive on the Preservation of NATO Digital Information of Permanent Value, especialmente en lo que afecta a los principios aplicables en la implementación de los sistemas de información en que se gestionan los documentos –**punto 2** de este anexo– y a la categorización de los tipos de contenido para preservación a largo plazo con objeto de establecer los formatos aplicables a su conservación –**punto 4** de este anexo–.

En casos de catástrofe y emergencias será de aplicación a la documentación de valor permanente conservada en el archivo electrónico del Ministerio de Defensa, lo establecido en el *Plan Nacional de Emergencias y Gestión de Riesgos en el Patrimonio Cultural.*

PRINCIPIOS A APLICAR EN LOS SISTEMAS QUE CONTIENEN INFORMACIÓN DE VALOR PERMANENTE

La preservación digital a largo plazo afecta a la información que reside dentro de los sistemas de información del Ministerio de Defensa. En el largo plazo no es necesario preservar la funcionalidad de los sistemas, solo los documentos contenidos en los mismos y la información contextual que permite documentar el entorno desde el que se originó la información. Los principios aplicables a los sistemas serán:

a) Sostenibilidad: los sistemas que contienen información de valor permanente serán desarrollados y mantenidos teniendo en cuenta la implicaciones de la gestión y preservación de dicha información en el corto medio y largo plazo.
b) Autenticidad: los sistemas que contienen información de valor permanente, deberán desarrollarse, implementarse y gestionar-

se de manera que se asegure la autenticidad y la integridad de los registros contenidos en el mismo.

c) Accesibilidad: los sistemas que contienen información de valor permanente deberán desarrollarse, implementarse y mantenerse para garantizar la accesibilidad a largo plazo de la información que contienen. Cualquier tipo de cifrado o contraseña deberán de ser eliminados cuando la información se traslada a los entornos de preservación a largo plazo.
d) Gestión del ciclo de vida: la información de valor permanente contenida en los sistemas del Ministerio de Defensa, deberá transferirse e incorporarse al archivo electrónico de acuerdo con los calendarios de conservación establecidos en el proceso de valoración.

Los requerimientos técnicos para los sistemas en que se conserven documentos de valor permanente se establecerán de acuerdo por el modelo tecnológico para la gestión documentos electrónicos del Ministerio de Defensa que se haya adoptado en el programa de tratamiento de los documentos previsto en el punto 2.7 de la política. En la actualidad, la práctica más extendida para el almacenamiento y gestión de dichos documentos consiste en el desarrollo de repositorios que adoptan el estándar *ISO 14721:2012 Space data and information transfer systems –Open archival information system (OAIS)– Reference model.* A dichos repositorios se transfiere la información digital y sus metadatos mediante paquetes estructurados SIP (*Submission Information Packages*) que son aceptados y almacenados por el archivo como AIP (*Archival Information Packages*) y se hacen disponibles para el acceso como DIP (*Disemination Information Packages*). En dicha norma se contienen además las recomendaciones para la auditoría de los repositorios digitales de confianza.

GRUPOS DE RIESGO Y MEDIDAS GENERALES DE CONSERVACIÓN

La siguiente tabla desarrolla los riesgos que pueden afectar a los documentos y se basa en la contenida en el anexo 9: Medidas a incluir en un plan de preservación, de la Política de Gestión de Documentos Electrónicos del Ministerio de Hacienda y Administraciones Públicas. Adicionalmente, y como referente en los trabajos de evaluación riesgos,

se podrá emplear el informe técnico UNE-ISO/TR 18128:2014 *Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental*.

Se identifican cinco grandes grupos de riesgo:

a) Los derivados de la evolución y obsolescencia tecnológica.
b) 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.
c) Los que proceden de una posible descontextualización de los documentos electrónicos.
d) 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.).
e) 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.

Grupo de riesgo	Riesgo	Recomendación
Obsolescencia	Soportes de almacenamiento	Sería necesario disponer de un catálogo de soportes, con indicación de su vida útil supuesta en condiciones óptimas y su antigüedad
	Formatos	Es importante conocer los errores o defectos conocidos de cada formato empleado
	Software	Se recomienda contar con la información acerca del historial de cambio de versiones y de la evolución prevista por los propios fabricantes
	Hardware	Se debería conocer, por ejemplo, la antigüedad del hardware, la posibilidad de disponer de piezas de recambio y la existencia de contratos de soporte y mantenimiento

Grupo de riesgo	Riesgo	Recomendación
Errores o fallos de la tecnología	Degradación de los soportes	Su causa puede deberse a una manipulación incorrecta de los mismos, a un almacenamiento que no se atiene a las indicaciones del fabricante en cuanto condiciones ambientales, al desgaste, etc.
	Corrupción o pérdida de datos	Determinados errores o la combinación de una serie de ellos podrían ocasionar alteraciones de la secuencia de bits en la que se almacenan los documentos electrónicos, lo que perjudicaría su legibilidad
	Fallo en los soportes o en el hardware	En este sentido es recomendable contar con el historial de fallos y errores de los soportes o el hardware, y sus causas.
		Asimismo es importante conocer el MTBF (meantime between failures, o tiempo medio entre fallos) de cada soporte, especificado por el fabricante del mismo
	Errores en las aplicaciones	Ya sean estas de desarrollo propio o aplicaciones comerciales, contando con la existencia en este caso de errores conocidos, deberían registrarse los errores sufridos y sus posibles causas
Descontextualización de los documentos	Ausencia de metadatos adecuados para la contextualización de los documentos electrónicos	Se requeriría establecer los controles necesarios para que los metadatos obligatorios se encuentren cumplimentados y el chequeo periódico del vínculo de los metadatos con sus correspondientes documentos
Seguridad	Ataques (internos o externos) que modifiquen o eliminen documentos electrónicos	Se aplicarán las medidas establecidas en materia de seguridad de la información

Grupo de riesgo	Riesgo	Recomendación
	Virus que puedan alterar los documentos o sus metadatos asociados	Se aplicarán las medidas establecidas en materia de seguridad de la información
	Robo (de soportes, especialmente en tránsito)	Se aplicarán las medidas establecidas en materia de seguridad de la información
Aumento de documentos y los costes asociados	Falta de espacio de almacenamiento	Deberían realizarse previsiones de crecimiento y de necesidades de almacenamiento. Se evitarían siempre la eliminación y los cambios de almacenamiento no controlados cuando se trate de documentos afectados por la PGDE-MINISDEF y muy especialmente aquellos de valor de conservación permanente.
	Rendimiento no ajustado a las necesidades de acceso de los sistemas de almacenamiento	Deberían realizarse previsiones de crecimiento y de necesidades de almacenamiento. Se evitarían siempre la eliminación y los cambios de almacenamiento no controlados cuando se trate de documentos afectados por la PGDE-MINISDEF y muy especialmente aquellos de valor de conservación permanente.
	Incapacidad de realizar copias de seguridad debido al volumen de los datos a salvar o exceder la ventana de backup (período de tiempo durante el cual se establece que se llevarán a cabo las copias de seguridad, sin que estas afecten al rendimiento de los sistemas o a las aplicaciones)	Deberían realizarse previsiones de crecimiento y de necesidades de almacenamiento. Se evitarían siempre la eliminación y los cambios de almacenamiento no controlados cuando se trate de documentos afectados por la PGDE-MINISDEF y muy especialmente aquellos de valor de conservación permanente.

En relación con las medidas de conservación, adoptadas en función del análisis de riesgos, estas se basarán en las detalladas en la norma *ISO/TR 18492:2005 «Conservación a largo plazo de información electrónica basada en documentos»*, y en las recomendaciones recogidas en la guía creada por el Grupo de Trabajo del Subcomité de

Gestión de documentos y archivos de ISO, responsable de la conservación de documentos electrónicos en el ámbito de la gestión documental (ISO - TC 46/SC 11 / WG 7). En general, parte de las medidas se basarían en alguno de los siguientes tipos:

a) Refresco o renovación (copia entre dos mismos tipos de soportes, sin cambio en los datos).
b) Migración (copia a otro tipo de soporte, sistema o formato).
c) Replicación (creación de un duplicado de los datos, como medio de protección ante la pérdida o degradación de los mismos).
d) Emulación (reproducir las funcionalidades de un sistema o soporte obsoletos).
e) Encapsulación (los documentos contienen en sí mismos todos los elementos que forman un objeto digital, p.e., los metadatos, las firmas asociadas y el propio documento).
f) Empleo de estándares abiertos no propietarios.

Un segundo conjunto de medidas tienen que ver con conceptos propios de los sistemas informáticos, como la alta disponibilidad, la redundancia de elementos para evitar los denominados puntos únicos de fallo, etc.

A continuación se detallan a modo de ejemplo, para cada tipo de riesgo identificado, una serie de medidas que podrían incluirse en un plan de preservación.

a) En cuanto a la obsolescencia:

    1.º De los soportes de almacenamiento:

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

    2.º De los formatos:

        i. Migración a un formato considerado longevo, especialmente en documentos de conservación permanente.
        ii. Uso de estándares y formatos abiertos, en vez de formatos propietarios.

3.º Del software:

i. Actualización de las versiones, según las recomendaciones de los fabricantes.

ii. Migración a otro tipo de software. Podría provocar cambios en los formatos de los documentos, lo que alteraría su integridad.

iii. Emulación: es una alternativa complicada y, seguramente, de elevado coste.

iv. Con objeto de que la obsolescencia del software no comprometa la conservación a largo plazo de los documentos electrónicos, podría ser recomendable reducir su dependencia de aplicaciones o bases de datos propietarias, al menos en la fase semiactiva o inactiva de la documentación, independizándolos de las mismas.
A continuación se exponen una serie de consideraciones en relación a este tipo de medidas.
Almacenar los documentos electrónicos en una base de datos presenta, en principio, algunas ventajas funcionales:

- Simplifica la administración.
- Facilita la salvaguardia de los datos, puesto que existen procedimientos y herramientas de backup específicamente orientados para estos entornos.
- Permite una transaccionalidad más sencilla.
- No hay necesidad de mantener enlaces externos entre los registros de la base de datos y los ficheros, con los riesgos potenciales de pérdida o modificación de rutas, renombrado accidental de ficheros, posibles agujeros de seguridad, etc.
- Los sistemas gestores de bases de datos (DBMS) proporcionan funcionalidades como la gestión de la integridad, control de accesos, trazabilidad, etc.

Por el contrario, el almacenamiento exclusivo de los documentos electrónicos en bases de datos propietarias supone un riesgo para la conservación a largo plazo de estos documentos debido a la obsolescencia segura del software.
Igualmente al tratarse de sistemas propietarios la migración de los documentos a otro software puede resul-

tar una operación costosa en recursos o difícil técnicamente, lo que podría comprometer la conservación de los mismos documentos almacenados.
Un tamaño excesivo de la base de datos que contiene los documentos electrónicos perjudicaría el rendimiento y la realización de copias de seguridad y podría comprometer su recuperación ante un desastre. En este caso, para reducir el tamaño y el tiempo de las copias de seguridad, al menos las que se realizan con más frecuencia, podrían emplearse métodos como el particionamiento de la base de datos:

- Las tablas que contienen documentos de un determinado rango de fechas se convierten en tablas de solo lectura y, por tanto, inmodificables.
- Las copias de seguridad podrían excluir estas tablas, reduciendo el volumen de los datos a salvar.
- Adicionalmente, estas particiones podrían almacenarse en soportes o sistemas de almacenamiento más económicos.

Una alternativa al almacenamiento de los documentos electrónicos en bases de datos podría ser su almacenamiento en sistemas de ficheros, independientes de estas mismas bases de datos. En este caso las bases de datos contendrían la ruta donde efectivamente se almacenan los documentos electrónicos.
Este sistema podría tener algunas ventajas frente al uso de bases de datos:

- Independizaría efectivamente a los documentos de bases de datos propietarias, lo que a largo plazo podría facilitar la conservación de esos documentos.
- Podría emplearse un tipo de soporte de almacenamiento más económico (p.e., discos duros de gran tamaño).
- Aunque depende de muchos factores, el acceso a los documentos podría llegar a ser más rápido.
- En función de la configuración de los sistemas gestores de bases de datos (DBMS), podría hacerse un uso más eficiente de la memoria, al necesitar menos para la recuperación de los documentos.

- Podría reducirse el tamaño de las copias de seguridad, al reemplazarlas por otros sistemas de protección propios de sistemas de almacenamiento como son las réplicas.

En todo caso, se presentan varias alternativas:

- Almacenar los documentos electrónicos firmados junto con sus metadatos en bases de datos como «Internal Binary Large Objects» (i-BLOB). Los i-BLOB son objetos de datos binarios de gran tamaño, que se almacenan directamente en tablas de la base de datos. Participan en el modelo transaccional típico de las bases de datos, garantizando las propiedades ACID (atomicidad, consistencia, aislamiento y durabilidad). El uso de este tipo de objetos binarios puede ocasionar la redundancia de los datos, al guardar varias veces un mismo objeto.
- Almacenar los metadatos en bases de datos y los documentos electrónicos firmados como «External Binary Large Objects» (e-BLOB). Los e-BLOB son objetos de datos binarios de gran tamaño que, al contrario que los i-BLOB, se almacenan en ficheros del sistema operativo fuera de las tablas de la base de datos. Son más eficientes para operaciones de lectura de objetos de tamaño muy grande. Asimismo su uso limita la posible redundancia de los objetos binarios puesto que permite referencias únicas a los mismos. No forman parte sin embargo de las transacciones de la base de datos, por lo que deberá ser el sistema de ficheros el que proporcione las garantías de integridad y el resto de propiedades ACID.
- Almacenar los metadatos en bases de datos y los documentos electrónicos firmados en sistemas de ficheros, manteniendo en aquellas únicamente los enlaces a los documentos. Este sistema tendría, frente a los dos anteriores, las ventajas y desventajas expuestas más arriba, y permitiría independizar el almacenamiento de los documentos electrónicos de los formatos propietarios de las bases de datos.

- Almacenar los metadatos y los documentos electrónicos firmados conjuntamente en sistemas de ficheros (como un objeto digital) y mantener una copia de los metadatos y el enlace a los documentos en la base de datos. Esta alternativa, variación de la anterior, facilitaría la realización de búsquedas. En este caso podría incluso llegar a guardarse en un campo de la base de datos el texto plano del documento.

Para seleccionar la alternativa más adecuada que garantice una serie de factores como la facilidad de administración, un rendimiento óptimo en cuanto a las necesidades de acceso, unas medidas de seguridad adaptadas a la naturaleza de la información contenida en los documentos y la integridad y conservación de esos documentos, habría que considerar su ciclo de vida y la fase de archivo en la que se encontrarían en cada momento.
Así pues, podría emplearse una estrategia que combine, para distintas series de documentos o fracciones de estas mismas series, cualquiera de las alternativas señaladas.

4.º Del hardware:

i. Migración, a otro hardware que, como hemos visto con el software, podría suponer cambios en los formatos de los documentos electrónicos.
ii. Emulación (aunque sería la opción menos recomendable por su coste y las complicaciones que supondría mantener sistemas que emulen las funcionalidades de otros sistemas).

b) En cuanto a errores o fallos de la tecnología:

1.º Sistemas RAID que aseguren los datos frente a fallos de los discos duros.
2.º Redundancia de los documentos mediante replicación:

i. La unidad mínima de replicación sería un volumen que contenga documentos electrónicos.
ii. Hay que indicar que un soporte de tipo cinta magnética corresponde a un volumen, mientras que en un

sistema de almacenamiento (con discos duros) pueden existir centenares o miles de volúmenes.

iii. En este sentido hay que recalcar la necesidad de tener bien localizados y ubicados los soportes, sean del tipo de sean, que contienen documentos electrónicos.

iv. En la misma línea podría ser recomendable no mezclar documentos electrónicos y otros tipos de datos no relacionados con ellos en los mismos soportes.

v. La replicación, por otro lado, se realizaría siempre entre soportes de la misma naturaleza, en cuanto tipo y capacidad.

vi. Para realizar las réplicas se emplearían las utilidades que suelen incorporar los mismos sistemas de almacenamiento o software especializado que permita hacerlas.

vii. La réplica, según su ubicación, podría ser de dos tipos:
- Remota, cuando su destino es un sistema de almacenamiento diferente situado en un edificio o ciudad distintos.
- Local, cuando es el mismo sistema de almacenamiento el que alberga las réplicas.

viii. Ambas formas de replicación no son incompatibles, por lo que en función de los recursos disponibles, del valor de los documentos electrónicos y de la necesidad de minimizar los posibles riesgos, podría ser recomendable combinarlas.

ix. Aun así sería preferible disponer, como mínimo, de una réplica remota.

x. Otro aspecto a determinar sería el número de réplicas que se consideran necesarias y su periodicidad. En este sentido habría que tener presente que las réplicas en disco, al ser más rápidas que las que se hacen a cinta magnética, por ejemplo, suelen reescribirse.

3.º Utilización de sistemas de almacenamiento de alta disponibilidad (doble controladora activo-activo, fuentes de alimentación redundadas, caché en mirror, etc.) que eviten puntos únicos de fallo y reduzcan las posibilidades de pérdidas de información.

4.º Técnicas de backup que permitan la recuperación de los documentos electrónicos a un estado previo.

5.º Almacenamiento de soportes de cinta magnética en condiciones ambientales controladas (armarios ignífugos, humedad, temperatura, etc., según recomendaciones de los fabricantes de los mismos soportes).
6.º Para documentos electrónicos digitalizados, en su fase semiactiva o inactiva, contar con un conjunto denominado «fichero maestro», en un formato considerado longevo (como TIFF, por ejemplo), a partir del cual se obtendrían las copias de consulta.
7.º Realizar comprobaciones periódicas de los distintos soportes, especialmente los de cinta magnética, para asegurarse de que mantienen todas sus propiedades y no presentan ningún tipo de degradación previa al final de su vida útil esperada.

c) En cuanto a la descontextualización de los documentos electrónicos:

1.º Uso de metadatos específicos de conservación, que aseguren la contextualización de los documentos electrónicos. En este sentido debería emplearse un estándar como los metadatos de preservación PREMIS.
2.º Considerar los documentos electrónicos como objetos digitales, mediante el encapsulamiento de los metadatos y los documentos en una misma estructura (por ejemplo, un fichero XML).
3.º Para documentos en fase semiactiva o inactiva almacenados en sistemas de ficheros, reproducción a este nivel del cuadro de clasificación de la organización.

d) En cuanto a la seguridad:

1.º Control de accesos.
2.º Control de soportes.

e) En cuanto al aumento de documentos y los costes asociados:

1.º Almacenamiento en capas (tiers) o jerárquico:

i. En función del número de accesos a los documentos se emplearían tipos de discos distintos, estableciendo un nivel jerárquico de mayor a menor rendimiento y de menor a mayor espacio de almacenamiento. De esta forma los documentos menos accedidos se ubicarían en discos más lentos y grandes y, por tanto, más económicos. El sistema en

tier o niveles aseguraría asimismo el rendimiento necesario en función de las necesidades de acceso a los documentos.

2.º Sistemas RAID adecuados a la naturaleza de los datos (RAID-1+0 para documentos muy accedidos o críticos; RAID-5 o RAID-6, que son más económicos, para documentos menos accedidos, por ejemplo).
3.º Uso de técnicas de duplicación en copias de seguridad a disco, con el objetivo de que el espacio necesario para el almacenamiento de las copias sea menor.
4.º Utilización de cintas magnéticas de gran capacidad para almacenar documentos en fase semiactiva (archivo central o intermedio), montando, por ejemplo, sistemas de ficheros en este tipo de soportes o empleándolos simplemente como sistema de backup o conservación permanente.
5.º Sistemas de archivado para reducir las licencias necesarias de copias de seguridad y permitir la utilización de sistemas de almacenamiento de gama inferior a los empleados para los documentos más accedidos:
    i. En este sentido se dispondrían de métodos como el particionamiento de las bases de datos y el empleo de tablas de solo lectura (ver medidas en relación a la obsolescencia del software), que reducen el volumen de las copias de seguridad y el tiempo necesario para realizarlas y permitirían emplear, si se considera oportuno, soportes de almacenamiento más económicos.

FORMATOS DE ARCHIVO PARA LA CONSERVACIÓN A LARGO PLAZO

Los siguientes formatos han sido tomados de la Directive on the Preservation of NATO Digital Information of Permanent Value y completados con los que figuran en la NTI de Catálogo de Estándares, cuando no coinciden, se ha hecho constar en nota al pie.

Se distinguen siete tipos de contenido principales con objeto de establecer los formatos adecuados para su preservación digital:

a) Conjuntos de datos (data sets).
b) Texto.

c) Imágenes fijas.
d) Imágenes en movimiento.
e) Sonido.
f) Información geoespacial.
g) Archivos Web.

En las tablas que se muestran a continuación se incluyen los formatos de archivo para mantenimiento a largo plazo, clasificados por tipo de contenido, incluyendo una breve descripción de los requisitos genéricos para su preservación.

Conjuntos de datos (Data sets)

Los *data sets* son colecciones de datos con valores individuales o de estructuras coherentes más grandes, como puedan ser los mensajes. Pueden ser resultado de una exportación desde base de datos o de un intercambio de información entre sistemas.

Por lo general, el conjunto de datos o *data set* tiene una estructura asociada, ya sea contenida implícitamente en el mismo (por ejemplo, una tabla de un documento Excel o base de datos) o explícitamente definido (por ejemplo, una definición de esquema).

Contenido	Requisitos	Formatos
Data sets (por ejemplo datos científicos) y cualquier estructura de información no acorde con otros tipos de contenido	▪ Preservar los datos estructurados y no estructurados para el análisis futuro ▪ Preservar la estructura lógica de los data set así como la sintaxis y semántica de los elementos contenidos en el mismo ▪ Preservar tipos y estructuras de datos	▪ IETF RFC 4180:2005, Formato común y MIME-Type para los ficheros separados por comas (Comma-Separated Values - CSV) ▪ Extensible Markup Language (XML), v1.1 2nd Edition, W3C. Recomendación, 29 de Septiembre de 2006. ▪ XML Schema Definition Language (XSD) 1.1 Parte 1: Estructuras and Parte 2: Tipos de datos, W3C. Recomendación, 5 de Abril de 2012.

Contenido	Requisitos	Formatos
Contenido de base de datos		▪ ISO/IEC 9075[7](Partes 1 a 14):2011, Información tecnología – Lenguajes de base de datos-- SQL.

Texto

Los documentos de texto pueden incluir también diagramas, imágenes o cualquier otro elemento no textual, que no deben ser separados del texto y se mantienen como parte del documento.

Contenido	Requisitos	Formatos
Documentos de texto, incluyendo los formatos comunes de Ms Office (docx, xlsx, pptx)	▪ Preservar la integridad del texto, diagramas e imágenes, paginación y navegación (formateando) ▪ Preservar los metadatos del documento ▪ Inclusión de fuentes, información de diseño e índices	▪ ISO 32000-1:2008, Document management - Portable document format - Part 1: PDF 1.7, conformance level : PDF/A-2a
Correo electrónico (por ejemplo ficheros MS Outlook PST)	▪ Preservar el contenido del correo electrónico incluyendo anexos ▪ Preservar los buzones completos. Los mensajes importantes pueden ser exportados y conservados como documentos de texto simples.	▪ IETF RFC 4155:2005[8], tipo de soporte de aplicación/mbox ▪ IETF RFC 2045[9], Multipurpose Internet Mail Extensions (MIME) ▪ IETF RFC 5321[9] Simple Mail Transfer Protocol (SMTP)

[7] Formato no incluido en «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».

[8] Formato no incluido en «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».

[9] Formato obtenido de «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».

Contenido	Requisitos	Formatos
Chat (por ejemplo conversaciones de JChat)	▪ Preservar el contenido de los mensajes incluyendo anexos ▪ Preservar las conversaciones completas por chat de usuario o multi-usuario con marcas de tiempo ▪ Preservar información sobre usuarios y grupos de usuarios	▪ ISO 32000-1:2008, Document management - Portable document format - Part 1: PDF 1.7, conformance level : PDF/A-2a ▪ IETF RFC 4155 :2005[8], tipo de soporte de aplicación/mbox ▪ IETF RFC 2045[9], Multipurpose Internet Mail Extensions (MIME) ▪ IETF RFC 5321[9], Simple Mail Transfer Protocol (SMTP)

Imágenes fijas

Las imágenes fijas son representaciones visuales, como fotografías, gráficos y diagramas, que pueden dividirse en dos tipos principales: imágenes de mapa de bits (raster) e imágenes vectoriales. Las imágenes de mapa de bits son normalmente fotografías generadas por escáneres y cámaras con una resolución fija, mientras las imágenes vectoriales se componen de objetos escalables. Ambos tipos pueden ser combinados.

Contenido	Requisitos	Formatos
Imágenes de mapa de bits/ raster	▪ Preservar la resolución (claridad, colores), escalabilidad y capacidad de renderizar la imagen ▪ Preservar los metadatos de la imagen ▪ Prioridad por la comprensión sin pérdidas ▪ Prioridad por resoluciones más grandes	▪ ISO/IEC 15444-1:2004, Information technology - JPEG 2000 image coding system., Parte 1 (J2K_C_LL, Core Coding, Lessless Compression) ▪ ISO/IEC 10918-1:1994[10], Information Technology –Digital compression and coding of continuous-tone still images ▪ Adobe TIFF UNC[10] (mapa de bits descomprimido), parte de TIFF 6.0 (1992) ▪ Adobe TIFF G4[10] (mapa de bits comprimido, parte de TIFF 6.0 (1992)

[10] Formato no incluido en «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».

Contenido	Requisitos	Formatos
		▪ ISO 12639:2004[11] Graphic technology - Prepress digital data exchange - Tag image file format for image technology (TIFF/IT)
Imágenes vectoriales		▪ W3C gráficos vectoriales escalables (Scalable Vector Graphics - SVG) 1.1, 2011

Imágenes en movimiento

Las imágenes en movimiento son grabaciones digitales de imágenes fijas a una velocidad y resolución particular. A menudo se aplica compresión solo con la captura de la diferencia entre tramas adyacentes. Las imágenes en movimiento se combinan normalmente con datos de audio y empaquetadas en un contenedor común.

Contenido	Requisitos	Formatos
Ficheros de vídeo	▪ Preservar la resolución (claridad, colores), escalabilidad y capacidad del vídeo ▪ Preservar los metadatos del vídeo, incluyendo códigos de tiempo y otras etiquetas ▪ Prioridad por la comprensión sin pérdidas ▪ Prioridad por resoluciones más grandes y bitrates de audio más altos	▪ ISO/IEC 13818-2:2000[12], Information technology – Generic coding of moving pictures and associated audio information: video / ITU T H.262 (MPEG-2) ▪ ISO/IEC 14496-2:2004[12] Information technology – Coding of audio-visual objects – Part 2: Visual / ITU-T H.263 (MPEG-4) ▪ ISO/IEC 14496-10:200312, Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding / ITU-T H.264 (MPEG-4 AVC)

[11] Formato obtenido de «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».

[12] Formato obtenido de «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».

Contenido	Requisitos	Formatos
		▪ ISO/IEC 14496-10:2009[13] Information technology - Coding of audio-visual objects - Part 10: Advanced Video Coding (H.264/MPEG-4 AVC) ▪ ISO/IEC 14496-14:2003[13] Information technology - Coding of audio-visual objects - Part 14: MP4 file format (MPEG-4 MP4 vídeo) ▪ WebM[13]

Sonido

Los archivos de sonido contienen grabaciones de voz u otro sonido. Esto incluye grabaciones de audio de reuniones si incluyen información de valor permanente.

Contenido	Requisitos	Formatos
Ficheros de sonido	▪ Preservar la resolución (frecuencia de muestreo) y la profundidad ▪ Preservar los metadatos de audio	▪ European Broadcast Union Tech 3285[14] – Especificación del Broadcast Wave Format (BWF) – Versión 2 (2011) (WAVE Audio with LPCM) ▪ ISO/IEC 11172-3:1993. Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s -- Part 3: Audio. 256 KB/s or higher

[13] Formato obtenido de «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».

[14] Formato no incluido en «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».

Contenido	Requisitos	Formatos
		– o bien – ▪ ISO/IEC 13818-3 (Second edition, 1998)[14]. Information technology -- Coding of moving pictures and associated audio information -- Part 3: Audio. 256 KB/s or higher (MPEG Layer III Audio Encoding) ▪ OGG Vorbis[15]

Geoespacial

La información geoespacial normalmente es producida, usada y contenida en sistemas de información geográfica (GIS). La información está relacionada con la categoría de imagen fija, puesto que la información geoespacial consta de mapas de bits o imágenes vectoriales más unos atributos adicionales asociados con localizaciones particulares descritas en los datos de la imagen.

Contenido	Requisitos	Formatos
Información geoespacial (por ejemplo datos GIS)	▪ Preservar la resolución y escalabilidad ▪ Preservar los metadatos geoespaciales	▪ OGC 07-147r2[16], Keyhole Markup Language (KML) 2.2.0, Abril de 2008 ▪ OGC 12-128r10[16], OGC GeoPackage Encoding Standard V1.0, 12 de Febrero de 2014

Archivo web

El tipo de archivo web se refiere al archivo de sitios web completos, portales o partes de ellos. Mientras alguna información puede estar

[15] Formato obtenido de «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».

[16] Formato no incluido en «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».

contenida en páginas web estáticas y, por lo tanto es fácil de capturar, otras partes pueden ser renderizadas dinámicamente.

Los archivos web normalmente contienen textos estructurados así como imágenes fijas y en movimiento.

Contenido	Requisitos	Formatos
Sitios web y portales	▪ Preservar estructura y contenido de la web, incluyendo scripts ▪ Podría ser necesaria la inclusión de contenido externo ▪ El contenido dinámico/ interactivo o específico de usuario es problemático	▪ ISO 28500:2009[17], Information and documentation – WARC file format ▪ IETF RFC 2557, MIME Encapsulation of Aggregate Documents, tal como HTML (MHTML)

EQUIVALENCIA ENTRE LOS METADATOS E-EMGDE Y PREMIS[18]

PREMIS se refiere a «unidades semánticas» donde este esquema (e-EMGDE) se refiere a «elementos de metadatos». Sin embargo, significan lo mismo, esto es, las características de los objetos digitales que tienen que ser descritas para asegurar que los objetos siguen siendo accesibles y utilizables a lo largo del tiempo.

En PREMIS, a todas las unidades semánticas por encima del nivel inferior de la jerarquía se hace referencia como «Contenedores». El e-EMGDE solo tiene tres niveles de jerarquía -elementos, sub-elementos y sub-sub-elementos-, aunque esto es extensible. PREMIS tiene jerarquías de contenedores y unidades semánticas que pueden llegar a cuatro niveles de profundidad.

En la siguiente concordancia, solo se muestran las unidades semánticas de PREMIS y su número de referencia. Se establece la con-

[17] Formato no incluido en «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».

[18] Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE). Documentación complementaria a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos. Ministerio de Hacienda y Administraciones Públicas

cordancia tanto para los tipos de entidad como para los niveles de elementos pertinentes.

Puesto que PREMIS es más amplio que e-EMGDE y tiene una orientación diferente, se propone un modelo de extensibilidad para la conservación de documentos, a efectos no prescriptivos, sino puramente informativos.

La siguiente tabla de concordancias es aproximativa y tiene valor informativo. Debe tenerse en cuenta que la orientación de e-EMGDE y de PREMIS son diferentes, el primero orientado hacia la gestión de documentos y la segunda orientada hacia la conservación. Se ha elaborado según la equivalencia incluida en la norma fuente Australian Government Recordkeeping Metadata Standard (AGRkMS).

PREMIS			e-EMGDE			
Entidad	**Nº**	**Unidad semántica**	**Entidad**	**Elemento**	**Sub-elemento**	**Sub-sub-elemento**
OBJETO	1.1.1	objectIdentifierType	**DOCUMENTO**	Identificador	Tipo de identificador	
	1.1.2	objectIdentifierValue		Identificador	Secuencia del identificador	
	1.2	objectCategory				
	1.3.1	preservationLevelValue				
	1.3.2	preservationLevelRole				
	1.3.3	preservationLevelRationale				
	1.3.4	preservationLevelDateAssigned				
	1.4.1	significantPropertiesType				
	1.4.2	significantPropertiesValue				
	1.4.3	significantPropertiesExtension				
	1.5.1	compositionLevel				
	1.5.2.1	messageDigestAlgorithm		Verificación de integridad	Algoritmo	
	1.5.2.2	messageDigest		Verificación de integridad	Valor	
	1.5.2.3	messageDigestOriginator				
	1.5.3	size		Características técnicas	Tamaño	Tamaño lógico

PREMIS			e-EMGDE			
Entidad	**Nº**	**Unidad semántica**	**Entidad**	**Elemento**	**Sub-elemento**	**Sub-sub-elemento**
				Características técnicas	Tamaño	Unidades
	1.5.4.1.1	formatName		Características técnicas	Nombre de formato	
	1.5.4.1.2	formatVersion		Características técnicas	Versión de formato	
	1.5.4.2.1	formatRegistryName		Características técnicas	Registro de formatos	
	1.5.4.2.2	formatRegistryKey				
	1.5.4.2.3	formatRegistryRole				
	1.5.5.1	creatingApplicationName		Características técnicas	Nombre de la aplicación de creación	
	1.5.5.2	creatingApplicationVersion		Características técnicas	Versión de la aplicación de creación	
	1.5.5.3	dateCreatedByApplication		Fechas	Fecha de inicio	
	1.5.5.4	creatingApplicationExtension				
	1.5.6.1	inhibitorType				
	1.5.6.2	inhibitorTarget				
	1.5.6.3	inhibitorKey				
	1.5.7	objectCharacteristicsExtension				
	1.6	originalName		Nombre	Nombre natural	
	1.7.1.1	contentLocationType				
	1.7.1.2	contentLocationValue		Ubicación	Localización	
	1.7.2	storageMedium		Ubicación	Soporte	
	1.8.1	environmentCharacteristic				
	1.8.2.	environmentPurpose				
	1.8.3	environmentNote				
	1.8.4.1	dependencyName				
	1.8.4.2.1	dependencyIdentifierType				
	1.8.4.2.2	dependencyIdentifierValue				

PREMIS			e-EMGDE			
Entidad	**Nº**	**Unidad semántica**	**Entidad**	**Elemento**	**Sub-elemento**	**Sub-sub-elemento**
	1.8.5.1	swName				
	1.8.5.2	swVersion				
	1.8.5.3	swType				
	1.8.5.4	swOtherInformation				
	1.8.5.5	swDependency				
	1.8.6.1	hwName				
	1.8.6.2	hwType				
	1.8.6.3	hwOtherInformation				
	1.8.7	environmentExtension				
	1.9.1.1	signatureEncoding		Firma		
	1.9.1.2	signer		Firma		
	1.9.1.3	signatureMethod		Firma		
	1.9.1.4	signatureValue		Firma		
	1.9.1.5	signatureValidationRules		Firma		
	1.9.1.6	signatureProperties		Firma		
	1.9.1.7	keyInformation		Firma		
	1.9.2	signatureInformationExtension		Firma		
	1.10.1	relationshipType	**RELACIÓN**	Categoría		
	1.10.2	relationshipSubType		Nombre	Nombre natural	
	1.10.3.1	relatedObjectIdentifierType				
	1.10.3.2	relatedObjectIdentifierValue		Entidad relacionada	ID de la entidad relacionada	
	1.10.3.3	relatedObjectSequence		Entidad relacionada	Rol de la relación	
	1.10.4.1	relatedEventIdentifierType		Identificador	Tipo de identificador	
	1.10.4.2	relatedEventIdentifierValue		Identificador	Secuencia del identificador	
	1.10.4.3	relatedEventSequence				
	1.11.1	linkingEventIdentifierType				

PREMIS			e-EMGDE			
Entidad	**Nº**	**Unidad semántica**	**Entidad**	**Elemento**	**Sub-elemento**	**Sub-sub-elemento**
	1.11.2	linkingEventIdentifierValue				
	1.12.1	linkingIntellectualEntityIdentifierType				
	1.12.2	linkingIntellectualEntityIdentifierValue				
	1.13.1	linkingRightsStatementIdentifierType	**DOCUMENTO**	Derechos de acceso, uso y reutilización	Tipo de acceso	
	1.13.2	linkingRightsStatementIdentifierValue		Derechos de acceso, uso y reutilización	Condiciones de acceso, uso y reutilización	
EVENTO	2.1.1	eventIdentifierType	**RELACIÓN**	Identificador	Tipo de identificador	
	2.1.2	eventIdentifierValue		Identificador	Secuencia del identificador	
	2.2	eventType		Categoría		
				Nombre	Nombre natural	
	2.3	eventDateTime		Fechas	Fecha de inicio	
				Fechas	Fecha de fin	
	2.4	eventDetail		Descripción		
	2.5.1	eventOutcome				
	2.5.2.1	eventOutcomeDetailNote		Trazabilidad	Historia del cambio	Valor anterior
	2.5.2.2.	eventOutcomeDetailExtension				
	2.6.1	linkingAgentIdentifierType				
	2.6.2	linkingAgentIdentifierValue		Entidad relacionada	ID de entidad relacionada	
	2.6.3	linkingAgentRole		Entidad relacionada	Rol de la relación	
	2.7.1	linkingObjectIdentifierType				
	2.7.2	linkingObjectIdentifierValue		Entidad relacionada	ID de la relación	
	2.7.3	linkingObjectIdentifierRole				

PREMIS			e-EMGDE			
Entidad	**Nº**	**Unidad semántica**	**Entidad**	**Elemento**	**Sub-elemento**	**Sub-sub-elemento**
AGENTE	3.1.1	agentIdentifierType	**AGENTE**	Identificador	Tipo de identificador	
	3.1.2	agentIdentifierValue		Identificador	Secuencia del identificador	
	3.2	agentName		Nombre		
	3.3	agentType		Categoría		
DERECHOS	4.1.1.1	agentType	**DOCUMENTO**			
	4.1.1.2	rightsStatementIdentifierValue				
	4.1.2	rightsBasis		Derechos de acceso, uso y reutilización	Tipo de acceso	
	4.1.3.1	copyrightStatus				
	4.1.3.2	copyrightJurisdiction				
	4.1.3.3	copyrightStatusDeterminationDate				
	4.1.3.4	copyrightNote				
	4.1.4.1.1	licenseIdentifierType				
	4.1.4.1.2	licenseIdentifierValue				
	4.1.4.2	licenseTerms		Derechos de acceso, uso y reutilización	Condiciones de acceso, uso y reutilización	
	4.1.4.3	licenseNote				
	4.1.5.1	statuteJurisdiction	**REGULACIÓN**	Jurisdicción		
	4.1.5.2	statuteCitation		Identificador	Secuencia del identificador	
	4.1.5.3	statuteInformationDeterminationDate				
	4.1.5.4	statuteNote				
	4.1.6.1	act	**AGENTE**	Seguridad	Permisos	
	4.1.6.2	restriction				
	4.1.6.3.1	startDate				
	4.1.6.3.2	endDate				
	4.1.6.4	rightsGrantedNote				
	4.1.7.1	linkingObjectIdentifierType				

PREMIS			e-EMGDE			
Entidad	**Nº**	**Unidad semántica**	**Entidad**	**Elemento**	**Sub-elemento**	**Sub-sub-elemento**
	4.1.7.2	linkingObjectIdentifierValue				
	4.1.8.1	linkingAgentIdentifierType				
	4.1.8.2	linkingAgentIdentifierValue				
	4.1.8.3	linkingAgentRole				
	4.2	rightsExtension				

ANEXO 6. Metadatos y tablas de valores de referencia relativos al acceso

METADATOS E-EMGDE RELATIVOS AL ACCESO Y SEGURIDAD

Por la especial relevancia que tienen para el Ministerio de Defensa, se incluyen los metadatos completos del e-EMGDE relativos al acceso y seguridad, que servirán de base para desarrollar el e-EMMDEF:

- e-EMGDE 8 SEGURIDAD
  - e-EMGDE 8.1 Clasificación de seguridad
    - e-EMGDE 8.1.1 Clasificación de acceso
    - e-EMGDE 8.1.2 Código de Política de control de acceso
  - e-EMGDE 8.2 Advertencia de seguridad
    - e-EMGDE 8.2.1 Texto de la advertencia
    - e-EMGDE 8.2.2 Categoría de la advertencia
  - e-EMGDE 8.3 Permisos
  - e-EMGDE 8.4 Sensibilidad datos de carácter personal
  - e-EMGDE 8.5 Clasificación ENS
  - e-EMGDE 8.6 – Nivel de clasificación de la información*
- e-EMGDE 9 DERECHOS DE ACCESO, USO Y REUTILIZACIÓN
  - e-EMGDE 9.1 – Tipo de acceso
    - e-EMGDE 9.1.1 – Código de la causa de limitación*
    - e-EMGDE 9.1.2 – Causa legal/normativa de limitación*
  - e-EMGDE 9.2 – Condiciones de reutilización

* Tomados del e-EMGDE en versión no publicada 20112014.

TABLA DE CODIFICACIÓN DE LAS RESTRICCIONES DE ACCESO

A continuación se muestran los criterios de codificación aplicables al metadato e-EMGDE 9.1.1. Código de la causa de limitación[19], que se emplean para identificar las causas legales por las que se puede producir una restricción de acceso:

Cod.	Código y contenidos de información con acceso restringido	Art. LTAIP
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	-

TABLA DE RÉGIMEN JURÍDICO DE ACCESO ESPECÍFICO

En caso de que las materias tengan previsto un régimen jurídico específico de acceso a la información se debe indicar la norma reguladora siguiendo

[19] Tomados del e-EMGDE en versión no publicada 20112014

los criterios del elemento e-EMGDE 9.1.2. Causa legal/normativa de limitación[20], tomando como referencia los incluidos en la siguiente tabla:

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.
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.

TABLA DE NIVELES DE SENSIBILIDAD DE DATOS DE CARÁCTER PERSONAL

Para los casos en los que existan datos de carácter personal protegidos por la LOPD, y no considerados «fuentes accesibles al público»

[20] Tomados del e-EMGDE en versión no publicada 20112014

se debe asignar un nivel de sensibilidad de datos de carácter personal empleando los siguientes criterios del elemento e-EMGDE 8.4 Sensibilidad de datos de carácter personal:

Valor	Datos de carácter personal	Disposición
Alto	Datos especialmente protegidos/sensibles/núcleo duro	15.1 LTAIP/ LOPD
Medio	Otros datos de carácter personal susceptibles de protección	15.3 LTAIP/LOPD
Bajo	Otros datos de carácter personal	LOPD

VALORES ESPECÍFICOS PARA EL ÁMBITO DE LA DEFENSA EN EL E-EMMDEF

En la elaboración del esquema de metadatos se tendrán que tener en cuenta los diferentes valores de los grados de clasificación aplicables en el ámbito de la defensa.

OTAN[21]	UE[22]	ESA[23]	e-EMMDEF
COSMIC TOP SECRET (CTS) / COSMIC TRÈS SECRET (CTS)	TRÈS SECRET UE / EU TOP SECRET (TS-UE/EU-TS)	ESA TOP SECRET (ESA TS)	SECRETO (S)
NATO SECRET (NS) / NATO SECRET (NS)	SECRET UE / EU SECRET (S-UE/EU-S)	ESA SECRET (ESA S)	RESERVADO (R)
NATO CONFIDENTIAL (NC) / NATO CONFIDENTIEL (NC)	CONFIDENTIEL UE / EU CONFIDENTIAL (C-UE/EU-C)	ESA CONFIDENTIAL (ESA C)	CONFIDENCIAL (C)
NATO RESTRICTED (NR) / NATO DIFFUSION RESTREINTE (NDR)	RESTREINT UE/EU RESTRICTED (R-UE/EU-R)	ESA RESTRICTED (ESA R)	DIFUSIÓN LIMITADA (DL)

[21] Grados de clasificación Organización del Tratado del Atlántico Norte (OTAN) en inglés o francés.

[22] Grados de clasificación Unión Europea (UE) en francés o inglés, o ambos simultáneamente (depende de la organización).

[23] Grados de clasificación Agencia Espacial Europea (ESA) en inglés.

PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO
DE ESPAÑA

MINISTERIO
DE DEFENSA

SECRETARÍA
GENERAL
TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL