



Eusko Jaurlaritzaren Informatika Elkarte
Sociedad Informática del Gobierno Vasco

Establecimiento de Políticas y Mecanismos de Conservación Documentos Electrónicos a Largo Plazo

Fecha: 15.7.2008

Referencia:

EstudioConservacionLargoPlazo_
v1.0

EJIE S.A.
Mediterráneo, 14
Tel. 945 01 73 00*
Fax. 945 01 73 01
01010 Vitoria-Gasteiz
Posta-kutxatila / Apartado: 809
01080 Vitoria-Gasteiz
www.ejie.es

Este documento es propiedad de EJIE, S.A. y su contenido es confidencial. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE, S.A.. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE, S.A. no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.



Control de documentación

Título de documento:

Histórico de versiones

Código: EstudioConservacionLargoPlazo

Versión: 1.0

Fecha: 15/7/08

Resumen de cambios:

Cambios producidos desde la última versión

Primera versión.

Control de difusión

Responsable: Antxon Larrañaga Uyarra

Aprobado por: Antxon Larrañaga Uyarra

Firma:

Fecha:

Distribución:

Referencias de archivo

Autor: Fernando Fdz. de Aránguiz

Nombre archivo: EstudioConservacionLargoPlazo_v1.0.doc

Localización: SharePoint Proyectos III

Contenido

Capítulo/sección	Página
1 INTRODUCCIÓN	5
2 ESTUDIO DE LA SITUACIÓN ACTUAL	7
2.1 Situación actual del Gobierno Vasco	7
2.1.1. Legislación	7
2.1.2. Archivo general	8
2.1.3. COVASAD	8
2.1.4. Modelo de Gestión Documental del Gobierno Vasco	9
2.1.5. Sistema de Gestión de Archivo (SGA)	11
2.1.6. Archivo digital	12
2.1.7. Formatos de documentos electrónicos del Gobierno Vasco	12
2.2 Buenas prácticas de otras organizaciones	13
2.2.1. Experiencias Internacionales	13
2.2.2. CATCert	13
2.2.3. Comisión de las comunidades europeas	14
2.2.4. Ministerio de Administraciones Públicas	15
2.3 Normativas técnicas	17
2.3.1. Modelos de gestión	18
2.3.2. Normativa técnica sobre conservación a largo plazo	23
2.3.3. Normativa sobre formatos de documentos electrónicos	25
2.3.4. Normativa técnica sobre descripción de documentos electrónicos	26
2.3.5. Requisitos para los sistemas de gestión de documentos electrónicos de archivo29	
2.3.6. Normativa técnica sobre firma electrónica	30
3 ESTUDIO DE REQUISITOS	31

3.1	Normativa legal	31
3.1.1.	Ley 30/1992. Procedimiento administrativo común	32
3.1.2.	Decreto 232/2000. Reglamento de los Servicios de Archivo	32
3.1.3.	Decreto 174/2003. Sistema de Archivo de la Adm. Pública de la CAE	33
3.1.4.	Ley 59/2003. Firma electrónica.	34
3.1.5.	Reglamento del sistema de archivo de la Adm. General de la CAE	35
3.1.6.	Comisión de Valoración, Selección y Acceso a la Documentación (COVASAD).	37
3.1.7.	Ley 11/2007. Acceso electrónico a los Servicios Públicos	37
3.1.8.	Decreto 232/2007, Utilización de medios electrónicos	40
3.2	Catálogo de requisitos	43
3.3	Catálogo de riesgos	43
4	PROPUESTAS DE ALTERNATIVAS DE SOLUCIÓN	45
5	PROPUESTA DE LA SOLUCIÓN	47
5.1	Políticas	49
5.2	Mecanismos	52
5.2.1.	Adquisición de documentos electrónicos	52
5.2.2.	Conservación de documentos electrónicos	55
5.2.3.	Acceso de documentos electrónicos	67
5.3	Ámbito de los mecanismos	68
5.4	Cobertura de los requisitos mediante los mecanismos	70
6	PLAN DE ACTIVIDADES	71
6.1	Ámbito normativo	71
6.2	Ámbito de difusión y comunicación	71
6.3	Ámbito organizativo	72
6.4	Ámbito técnico	72

7	ANEXOS	73
7.1	Normativa jurídica relativa a la facturación electrónica	73
7.1.1.	Facturación telemática y conservación electrónica de facturas	73
7.1.2.	Expedición de facturas electrónicas a la Administración General del Estado.	74
7.2	Formatos de avanzados de firma electrónica	75
7.3	Glosario	78
7.4	Bibliografía y Referencias	90

1 INTRODUCCIÓN

Contexto del estudio

El objeto del presente documento es plasmar el resultado del estudio realizado por el grupo de trabajo Proyectos III relativo al “**Establecimiento de Políticas y Mecanismos de Conservación Documentos Electrónicos a Largo Plazo**”.

Este estudio se enmarca en el proyecto “**Desarrollo y evolución de la plataforma ECM**”. Este proyecto es continuación del proyecto “**Sistema de Gestión Documental con Archivo Digital**” que, entre otras recomendaciones, apuntaba la necesidad de “*incorporar en el SGA (Sistema de Gestión de Archivo del Gobierno Vasco) procedimientos y herramientas de conservación a largo plazo de los documentos electrónicos*”.

Motivos del estudio

La producción administrativa del Gobierno Vasco genera documentos. Estos documentos son evidencia jurídica y memoria histórica de la actividad del Gobierno Vasco. Por tan motivo, es obligación del Gobierno Vasco conservarlos y mantenerlos disponibles.

Desde el momento en que el Gobierno Vasco habilita la teletramitación, dispone sólo de originales electrónicos del proceso. A partir de ese momento, la conservación de los documentos electrónicos es un deber ineludible.

La conservación a largo plazo de los documentos electrónicos es una preocupación reciente que trata de garantizar que los documentos electrónicos sigan siendo evidencia jurídica y memoria histórica de la actividad del Gobierno Vasco más allá del tiempo que perdure la tecnología que creó y/o firmó dichos documentos. Este es el motivo que ha llevado a la realización del presente estudio.

Ámbitos del estudio

Este estudio se ha realizado teniendo en cuenta tres ámbitos complementarios:

- El ámbito **tecnológico** es el que, por una parte, nos permite la gestión de documentos en soporte electrónico y, por otra, nos plantea importantes problemas para la conservación de dichos documentos (integridad de los documentos, obsolescencia de los soportes, vulnerabilidad de los sistemas de firma electrónica, etc.).
- El ámbito **jurídico** ha llegado recientemente a un nivel óptimo de desarrollo en materia de gestión de documentos electrónicos, quizás no tanto en cuanto a su conservación de su valor probatorio, quedando pendiente la práctica cotidiana de su aceptación procesal.
- El ámbito **archivístico**, competencialmente el responsable de la conservación de los documentos, históricamente ha aportado los mecanismos de conservación de documentos en soporte papel (identificación valoración, selección, etc.), apoyándose en el ámbito tecnológico y jurídico, debe ampliarlos para adaptarlos también a los soportes electrónicos.

Objetivo del estudio

El objetivo del presente estudio es establecer las políticas y mecanismos de conservación de documentos electrónicos a largo plazo que amplíen y se complementen con las ya existentes –bien fundamentadas en sólidos principios archivísticos- para los documentos en soporte papel.

Metodología del estudio

Para realizar el estudio de la conservación de documentos electrónicos a largo plazo se han realizado las siguientes actividades.

En primer lugar se ha estudiado la **situación actual del Gobierno Vasco**: Legislación, Modelo de Gestión Documental, Archivo general, COVASAD, Sistema de Gestión de Archivo (SGA), Archivo digital y Formatos de documentos electrónicos.

Después se enumeran un conjunto de **buenas prácticas en otras organizaciones**: EEUU, Australia, Provincia de Victoria (Australia), Colaboración Internacional, CATCert, Comisión de la comunidades europeas, y MAP.

Después se enumeran las **normativas técnicas** (Gestión, conservación a largo plazo, formatos de documentos electrónicos, descripción de documentos electrónicos, requisitos para los sistemas de gestión y firma electrónica) y se citan sus partes más relevantes en materia de conservación documentos electrónicos a largo plazo.

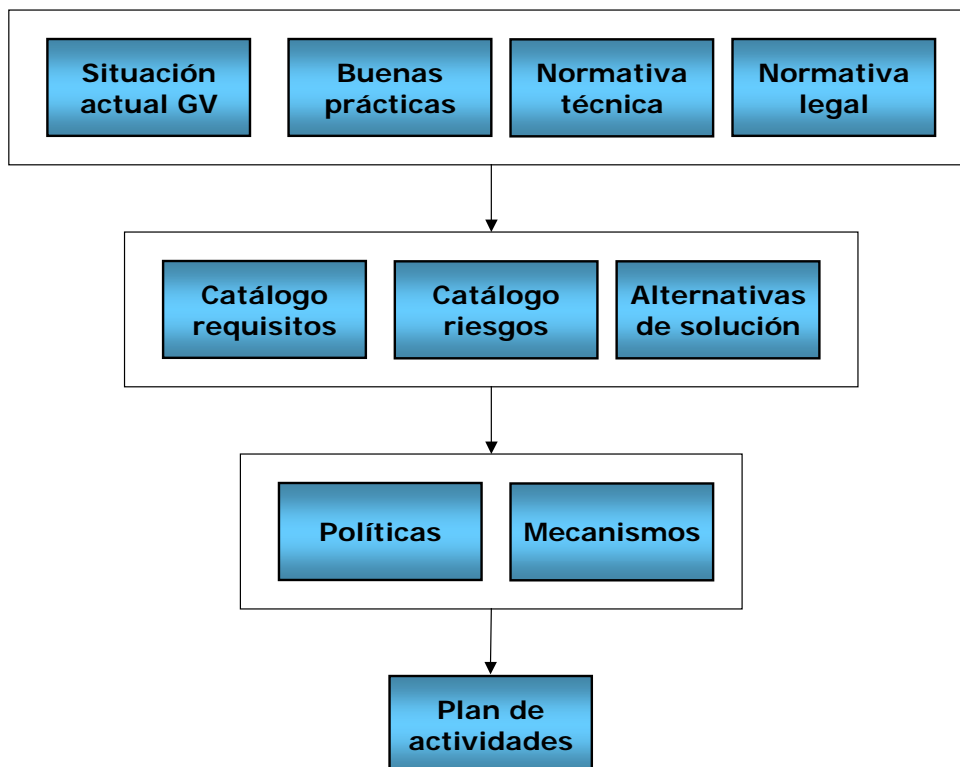
Después se enumeran las **normativas legales** y se citan sus partes más relevantes en materia de conservación documentos electrónicos a largo plazo.

En base a los cuatro elementos anteriores se establecen:

- **Catálogo de requisitos**: Autenticidad, Integridad, Disponibilidad, Confidencialidad
- **Catálogo de riesgos**
- **Alternativas de solución**

A partir de los requisitos, los riesgos y las alternativas de solución se establecen y describen las **políticas** y **mecanismos** de conservación de documentos electrónicos a largo plazo.

Finalmente, se propone un **plan de actividades** para desarrollar e implantar las políticas



2 ESTUDIO DE LA SITUACIÓN ACTUAL

El estudio de la situación actual se ha dividido en tres apartados:

1. Situación actual del Gobierno Vasco
2. Buenas prácticas de otras organizaciones
3. Normativas técnicas

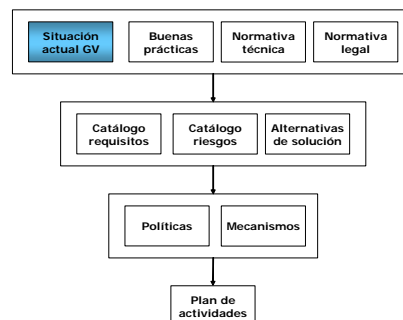
2.1 Situación actual del Gobierno Vasco

En el Gobierno Vasco la conservación a largo plazo de los documentos es una función que ejerce el Archivo general. Para ello se apoya en el Sistema de Gestión de Archivo (SGA). Esta función se ejerce fundamentalmente sobre los documentos en soporte papel ya que hasta hace unos años era casi el único soporte.

El uso generalizado de la documentación electrónica ha llevado al Gobierno Vasco a implantar una herramienta corporativa de gestión documental, el Archivo digital.

Los documentos electrónicos, en materia de conservación a largo plazo, tienen unas particularidades que hasta ahora no estaban contempladas en las políticas y mecanismos de conservación a largo plazo del Gobierno Vasco. Es por esto que se está realizando este estudio.

Son relevantes en materia de conservación de documentos electrónicos los siguientes elementos:



Desde un punto de vista Jurídico	<ul style="list-style-type: none"> • Legislación • Modelo de Gestión Documental
Desde un punto de vista Archivístico	<ul style="list-style-type: none"> • Archivo General • COVASAD
Desde un punto de vista Técnico	<ul style="list-style-type: none"> • Sistema de Gestión de Archivo (SGA) • Archivo digital • Formatos de documentos electrónicos

2.1.1. Legislación

En el estudio se ha tenido en cuenta la siguiente legislación de la CAE:

- Decreto 232/2000, de 21 de noviembre, por el que se aprueban el Reglamento de los Servicios de Archivo y las normas reguladoras del Patrimonio Documental del País Vasco.
- Decreto 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi.
- Orden de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.
- Orden de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, sobre el procedimiento para la identificación y valoración documental, y el funcionamiento de la Comisión de Valoración, Selección y Acceso a la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi (COVASAD).
- Decreto 232/2007, de 18 de diciembre, por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos

2.1.2. Archivo general

El Archivo general es uno de los subsistemas del Sistema de Archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi

Recibe y gestiona la documentación remitida por los archivos de gestión o de oficina y por los archivos centrales de la Administración Institucional, una vez finalizado el plazo de permanencia en estos archivos. Asimismo recibirá la documentación remitida por la Administración del Estado o por las Administraciones Forales en virtud del traspaso de competencias a la Comunidad Autónoma de Euskadi.

Este archivo, según el reglamento de Archivo, realiza las siguientes **funciones** principales en relación a la gestión y tratamiento de la documentación de archivo a largo plazo:

La realización del **expurgo de la documentación** en los plazos previstos en el Calendario de Conservación de la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi.

La **conservación** y custodia **de los fondos documentales** existentes durante el plazo de permanencia de la documentación en el Archivo General.

La **transferencia al Archivo Histórico** de aquella documentación para la que se establece su conservación permanente.

Participación activa en los procesos de **identificación y valoración de la documentación**, de los que resultan:

1. 1.– **El Calendario de Conservación** de la Documentación de la Administración General a Institucional de la Comunidad Autónoma de Euskadi.
2. 2.– La concreción de los **plazos de permanencia** de las series documentales en los archivos del Sistema y, con ello, la programación de las transferencias periódicas de documentación.
3. 3.– La concreción de los **criterios de accesibilidad** que afecta a la documentación de la Administración.

2.1.3. COVASAD

La COVASAD es la Comisión de Valoración, Selección y Acceso de la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi.

La COVASAD se configura como un órgano asesor, de carácter participativo e interdisciplinar, con las funciones de analizar y **valorar** todas las tipologías y series documentales generadas por la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

La **valoración documental** es el proceso necesario para establecer el **Calendario General de Conservación**, instrumento básico para **racionalizar la conservación de los fondos documentales** y, por ende, el patrimonio documental.

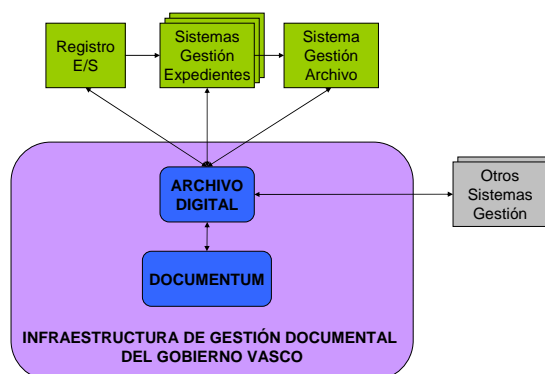
El Calendario General de Conservación constituye el instrumento de gestión en el que se describen la totalidad de las series documentales existentes, proporcionándose por cada una de ellas la siguiente información:

Código de la clasificación, Denominación normalizada de la serie, Unidad administrativa productora, **Soporte**, **Periodo de permanencia en los distintos niveles de archivo** (en años naturales), **Tipo de conservación**, Tipo de muestra a conservar, **Régimen de acceso** a la documentación y Orden de aprobación del calendario de conservación (fecha y número del BOPV).

2.1.4. Modelo de Gestión Documental del Gobierno Vasco

El Modelo de Gestión Documental (MGD) es un esquema teórico que facilita la comprensión y la homogénea implantación de la Gestión documental corporativa del Gobierno Vasco. Es una propuesta de sistematización de la Gestión documental corporativa del Gobierno Vasco. Describe y concreta las funciones, procesos y roles en materia de Gestión documental con el objetivo final de contribuir a la eficacia organizativa.

El siguiente esquema detalla la arquitectura del MGD basada en un Archivo digital que presta servicios de gestión documental a los sistemas de producción administrativa (Registro de Entrada/Salida, Sistemas de Gestión de Expedientes y el Sistema de Gestión de Archivo) y, también, al resto de sistemas de gestión que necesiten funcionalidades documentales. El Archivo digital es un conjunto de servicios documentales que se apoyan en la herramienta Documentum.



La conservación a largo plazo en el MGD

La mayoría de los documentos electrónicos custodiados por el SGA perdurarán a la tecnología de las herramientas que los crearon.

Por tal motivo el SGA debe incorporar procedimientos y herramientas de conservación a largo plazo de los documentos electrónicos.

El "Reference model for an Open Archival Information System" (OAIS), ISO 17421, ofrece el marco para definir un **sistema de archivo digital orientado a la conservación a largo plazo**, proporcionando la conceptualización y la terminología para establecer los elementos, las fases y el funcionamiento de este archivo.

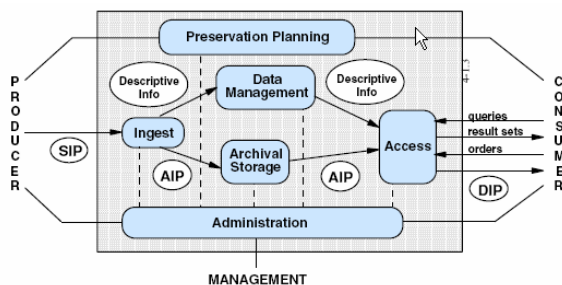
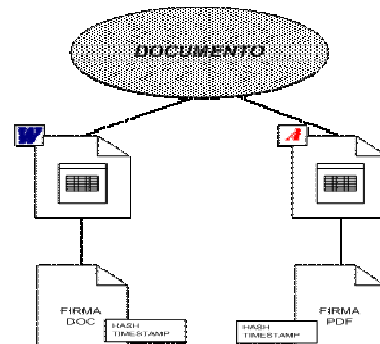


Figure 4-1: OAIS Functional Entities

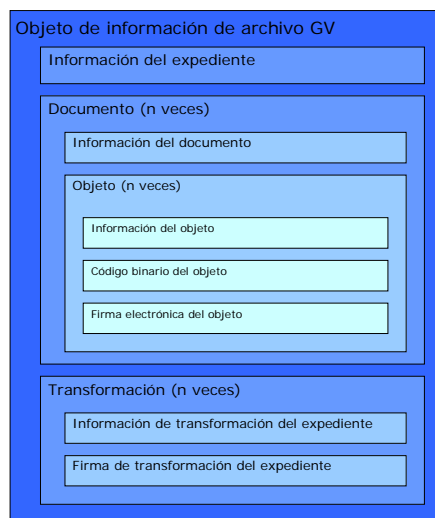
Adaptando OASIS a las particularidades del Gobierno Vasco se propone lo siguiente:

En el SGA, en el nivel de archivo de oficina, ingresarán los documentos electrónicos en formato original con su firma (si la tuvieran).

Cuando lo determinen los calendarios de conservación, los expedientes se transferirán al Archivo general. Como paso primero firmarán el documento "Relación de transferencia al Archivo general" el/la Jefe del Archivo general y el/la Depositario del departamento remitente. Después se transferirá la documentación tanto en soporte papel como en soporte electrónico. De cada documento electrónico transferido (en su formato original) se realizará una copia en el formato de conservación a largo plazo. Esta copia estará firmada por el Archivo general prolongando, de esta manera, su valor probatorio y evidencial.



Con la información de cada expediente transferido al Archivo General, sus metadatos y documentos electrónicos, se generará un objeto conservable "Objeto de información de archivo de GV" (Archival Information Package, AIP, según el modelo OASIS - - ISO 14721) que será almacenado por el SGA como soporte de conservación a largo plazo y que tendrá la siguiente estructura (codificada en formato XML):



A partir de ese momento, cuando el usuario solicite la visualización de un documento, el SGA ofrecerá ambos documentos (original y copia-largo-plazo) al interesado.

Tras el paso de los años, cuando el documento original quede obsoleto, el Archivo general seguirá garantizando la legibilidad del documento copia-largo-plazo. Para ello, periódicamente, realizará tareas de:

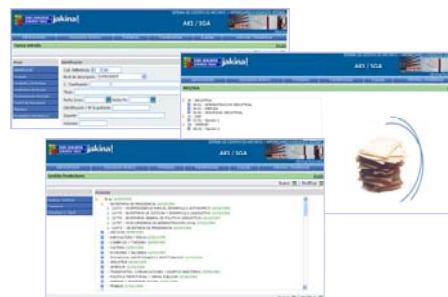
- Chequeo de errores
- Revisión de la legibilidad
- Migración
- Emulación
- Actualización de la firma electrónica
- ...

2.1.5. Sistema de Gestión de Archivo (SGA)

El SGA es el sistema que gestiona la conservación y el acceso a la información a lo largo del tiempo. Automatiza los procesos de Archivo.

Las funcionalidades principales del SGA son:

- Registro y Descripción de Archivo en base a una descripción multinivel
- Consulta de información por criterios múltiples
- Gestión de cuadros de clasificación de fondos
- Gestión de estructuras organizativas productoras
- Transferencia de documentación entre distintos niveles de archivos
- Control y Gestión de Préstamos, consultas y reproducciones
- Control y Gestión de espacios de archivo
- Gestión de Expurgo
- Gestión de los documentos electrónicos (se almacena en el Archivo digital)
- Gestión de los calendarios de conservación



KONTSERBATZEKO EGUTEGI OROKORRA CALENDARIO GENERAL DE CONSERVACIÓN												
Salikapen-kodea Código Clasificación	Segida Serie	Unitate ekolotza Unidad Productora	Euskarria Soporte	Artxiboan eman beharreko denbora Permanencia en Archivo			Kontserbazio-mota Tipo de conservación		Lagin-mota Tipo de muestra	Dokumentaziora jotzeko erabilera Régimen Acceso	Onespen-agindua Orden de aprobación	Txosten-zk. Nº Dossier
				Bulegoa artxiboan Archivo Oficina	Erakundeko artxibo zentralan Archivo Central Institucional	Artxibo Nagusian Archivo General	Osoa Total	Zati bat Parcial				

Informe del Calendario general de conservación (extraído el reglamento)

Identificación

Título: IN.01.01 - Actas de inspección metrología de Alava

Descripción:

Nivel de Descripción: SERIE

Documentos que componen el Expediente:

Conservación

Expurgo Total

Muestreo:

Plazo de Expurgo: 1

Permanencia en años por Nivel de Archivo

ARCHIVO DE OFICINA: 1

ARCHIVO CENTRAL INSTITUCIONAL:

ARCHIVO GENERAL:

ARCHIVO HISTÓRICO:

Régimen y Condiciones de Acceso

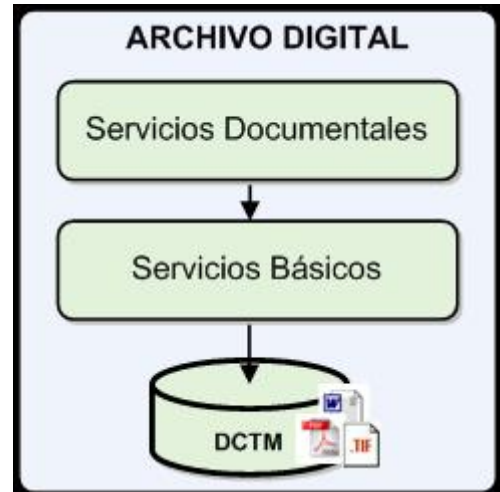
Ficha de un calendario de conservación en el SGA

2.1.6. Archivo digital

El Archivo digital, como hemos visto en el Modelo de Gestión Documental del Gobierno Vasco, es el componente corporativo que ofrece a los sistemas de información corporativos servicios documentales.

Características principales:

- Repositorio Común de documentos electrónicos
- Control de Acceso a Documentos (XLNets, ACL's)
- Conservación de Documentos
- Cumplimiento de LOPD
- Gestión de Auditorias
- Independencia de la Plataforma
- Arquitectura SOA. Servicios Gestión Documental:
 - Servicios Documentales (almacenamiento, búsquedas,...)
 - Servicios de Transformación de formato (conservación a largo plazo,...)
- Requisitos (Decreto de Medios EIT en los Procedimientos Administrativos)
 - Autenticidad, Integridad, Disponibilidad, Confidencialidad, Conservación.



2.1.7. Formatos de documentos electrónicos del Gobierno Vasco

2.1.7.1. Riesgos identificados para la definición de los formatos estandarizados de los documentos electrónicos

Obsolescencia tecnológica de los aplicativos que leen los documentos electrónicos

Los actuales y los futuros formatos de documentos electrónicos, probablemente, perdurarán a los aplicativos que los crearon y permiten visualizarlos. Por tal motivo, es fundamental definir unos formatos de conservación a largo plazo y definir e implementar unas políticas y procedimientos de conservación a largo plazo.

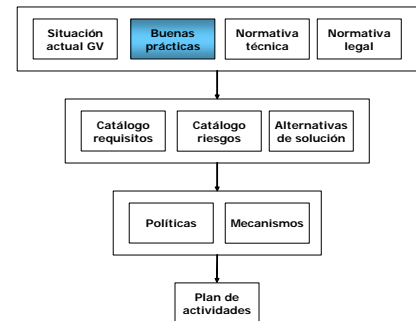
Este riesgo será estudiado en el subproyecto "Establecimiento de Políticas y Mecanismos de Conservación Documentos Electrónicos a Largo Plazo". En dicho subproyecto se propondrán las medidas necesarias para controlar dichos riesgos.

2.1.7.2. Formatos de documentos electrónicos en el escenario de almacenamiento:

Almacenar los documentos electrónicos **en el mismo formato en el que se reciben** por parte del ciudadano o que se generan dentro de la propia organización

Como **formato de conservación a largo plazo** de los documentos electrónicos almacenados se recomienda la utilización el **PDF/A**

2.2 Buenas prácticas de otras organizaciones



2.2.1. Experiencias Internacionales

Las principales experiencias internacionales en conservación de documentos electrónicos a largo plazo son:

PAÍS	Proyecto
EEUU	Electronic Records Archives (ERA) ¹
Australia	Strategies to ensure records remain accessible in the long term ²
Provincia de Victoria (Australia)	Digital Archive Project ³
Reino Unido	CEDARS ⁴
Colaboración internacional	InterPARES ⁵

2.2.2. CATCert

El proyecto iArxiu⁶, es un servicio de archivo electrónico que CATCert ofrecerá a las administraciones públicas catalanas. Esta plataforma debe permitir a las administraciones públicas poder depositar cualquier objeto digital y CATCert les garantizará que el apoyo no será ningún problema para su recuperación.

Ofrecerá servicios de archivo electrónico en fase semiactiva e histórica

Asumirá la responsabilidad del mantenimiento de

- Disponibilidad
- Preservación
- Evidencia

de documentos electrónicos durante largos periodos de tiempo más allá de la obsolescencia tecnológica.

La versión 2.0 de iArxiu estará operativa a partir de diciembre de 2008.

2.2.3. Comisión de las comunidades europeas

2.2.3.1. DECISIÓN DE LA COMISIÓN de 7 de julio de 2004 por la que se modifica su Reglamento interno (2004/563/CE, Euratom)

Artículo 2

Ámbito de aplicación

Las presentes disposiciones se aplicarán a los documentos electrónicos y digitalizados elaborados o recibidos y conservados por la Comisión.

Artículo 7

Conservación

1. La conservación por la Comisión de los documentos electrónicos y digitalizados deberá estar garantizada durante todo el período de conservación exigido, en las siguientes condiciones:

- a) el documento se conservará en la forma en que haya sido elaborado, enviado o recibido, o en una forma que preserve la integridad no sólo del contenido del documento, sino también de los metadatos que lo acompañan;
- b) el contenido del documento y los metadatos que lo acompañan deberán ser legibles durante todo el período de conservación por cualquier persona que tenga autorizado el acceso;
- c) en el caso de un documento enviado o recibido por vía electrónica, los datos que permiten determinar su origen y destino, así como la fecha y la hora de envío o recepción, formarán parte de los metadatos mínimos de obligada conservación;
- d) en el caso de procedimientos electrónicos gestionados por sistemas informáticos, los datos relativos a las etapas formales del procedimiento deberán conservarse en condiciones que permitan garantizar tanto la definición de estas etapas como la identificación de los autores y participantes.

2. A los efectos de lo dispuesto en el apartado 1, la Comisión creará un sistema de depósito electrónico destinado a cubrir el conjunto del ciclo de vida de los documentos electrónicos y digitalizados.

2.2.3.2. SEC(2005)1578 - "Electronic and digitised documents" - Implementing rules for the provisions on electronic and digitised documents (Decision 2004/563/EC, Euratom) :

La Comisión Europea especifica los formatos a utilizar en los documentos electrónicos y digitalizados de original en papel, dentro del procedimiento del Euratom.

Los documentos serán digitalizados en un formato que garantice la **permanencia** y **legibilidad** a lo largo del tiempo. El formato de digitalización de los documentos en papel será:

a) PDF o PDF/A

ó

b) TIFF con una resolución mínima de 300 dpi.

Estos formatos se enriquecerán con un procedimiento de OCR, para facilitar las búsquedas de texto, pero manteniendo la imagen sin modificación.

Cuando los documentos digitalizados sean transferidos al repositorio definitivo o archivo histórico, se todos los formatos se convertirán a PDF/A (ISO 19005) o un formato equivalente que garantice la conservación a largo plazo.

2.2.4. Ministerio de Administraciones Públicas

El Ministerio de Administraciones Públicas publicó en el año 2004 un documento, “**Criterios de conservación**”⁷, elaborado por el Consejo Superior de Informática y para el impulso de la Administración Electrónica, expone los **requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico** en las aplicaciones cuyo resultado sea utilizado para el ejercicio por los órganos y entidades del ámbito de la Administración General del Estado de las potestades que tienen atribuidas.

El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, modificado por el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, encomienda al Consejo Superior de Informática y para el Impulso de la Administración Electrónica la aprobación y difusión de los **criterios de conservación de la información** en el marco de las aplicaciones que efectúen tratamientos de información cuyo resultado sea utilizado por los órganos y entidades del ámbito de la Administración General del Estado para el ejercicio de las potestades que tienen atribuidas.

Los ‘Criterios de conservación’ de las aplicaciones utilizadas para el ejercicio de potestades tienen por objetivo:

- Proporcionar el conjunto de **medidas organizativas y técnicas** de seguridad que garanticen el cumplimiento de los requisitos legales para la conservación de la información en soporte electrónico relativa a los procedimientos administrativos de la Administración General del Estado que utilicen los medios electrónicos, informáticos y telemáticos en el ejercicio de sus potestades.
- Facilitar la adopción generalizada por parte de la Administración General del Estado de medidas organizativas y técnicas que **aseguren la conservación de la información** manejada por las aplicaciones utilizadas para el ejercicio de potestades.
- Promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa y asegurar a la vez el **respeto de las garantías y derechos de los ciudadanos** en sus relaciones con la Administración

El documento se estructura en los siguientes capítulos:

- Conservación de la información en soporte electrónico
- Ciclo de vida de la información en soporte electrónico
- Formato de la información en soporte electrónico
- Soportes
- Medidas de almacenamiento y conservación
- Sistema de archivos

Para cada uno de estos capítulos se tratan los siguientes aspectos:

- Las prescripciones o requisitos legales, que obligan a aplicar las distintas medidas para la conservación de la información, en particular en relación con la validez de los procedimientos administrativos y con los datos de carácter personal.
- Los criterios señalan las medidas de seguridad organizativas y técnicas que se deben adoptar para satisfacer los requisitos anteriores; además, se numeran para facilitar su localización y referencia.
- Las recomendaciones complementan a los criterios expuestos con otras medidas técnicas u organizativas posibles.
- Los niveles de seguridad desarrollan los niveles de seguridad a los que se refiere el Real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de

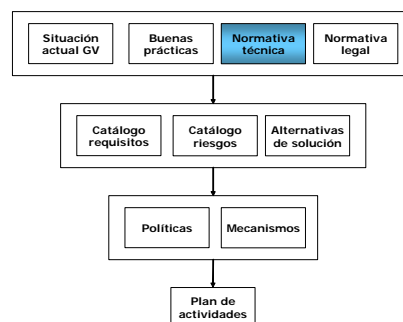
carácter personal y que se aplican a los criterios. No obstante, las medidas necesarias para garantizar la seguridad que deben reunir los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervienen en el tratamiento y conservación de los datos de carácter personal, están expuestas con más detalle en el documento 'Criterios de seguridad'.

- La ampliación técnica da referencias que permiten profundizar y ampliar los conceptos técnicos y organizativos en los que se fundamentan las distintas medidas de conservación.

2.3 Normativas técnicas

En materia de conservación documentos electrónicos a largo plazo estas son las principales normas técnicas:

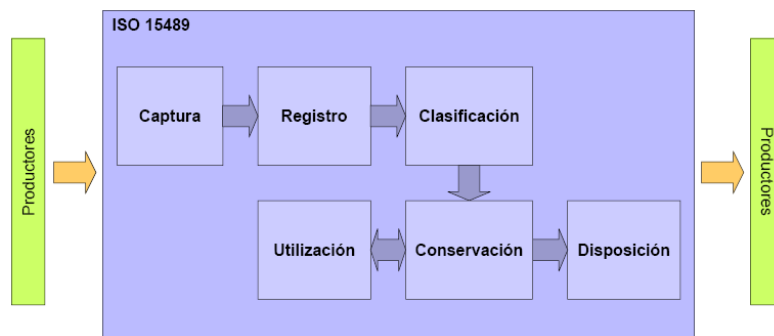
- **Modelos de gestión**
 - ISO 15489-1
 - ISO 15489-2
 - ISO 14721 (OAIS)
- **Normativa técnica sobre conservación a largo plazo**
 - ISO/TR 18492
 - ISO/PDTR 26102
- **Normativa sobre formatos de documentos electrónicos**
 - ISO 19005 (PDF-A)
- **Normativa técnica sobre descripción de documentos electrónicos**
 - ISO 23081
 - ISAD
 - METS
 - PREMIS
- **Requisitos para los sistemas de gestión de documentos electrónicos de archivo**
 - Moreq
 - DoD 5015.2
- **Normativa técnica sobre firma electrónica**



2.3.1. Modelos de gestión

- ISO 15489-1
- ISO/TR 15489-2
- ISO 14721 (OAIS)

2.3.1.1. ISO 15489-1:2001. Information and documentation – Records management – General.



Los principales puntos de esta norma técnica en materia de conservación de documentos electrónicos a largo plazo son:

8.3 Diseño e implementación de un sistema de gestión de documentos

8.3.5 Conversión y migración. Los sistemas de gestión de documentos se deberían diseñar de manera que se garantice la **autenticidad**, la **fiabilidad** y el uso de los documentos, **aunque se produzcan cambios en el sistema, incluyendo la conversión del formato**, la migración entre hardware y sistemas operativos o aplicaciones específicas de software **durante todo el periodo de conservación**.

8.5 Suspensión de los sistemas de gestión de documentos

Cuando un sistema de gestión de documentos se suspende o finaliza no se pueden añadir más documentos al sistema, aunque los que contiene deberían seguir siendo **accesibles**. Los documentos pueden retirarse del sistema de acuerdo con las directrices vigentes sobre conservación y disposición o mediante estrategias de **conversión y migración**. El proceso de suspensión de sistemas debería documentarse con el detalle necesario para mantener la **autenticidad, fiabilidad, integridad y disponibilidad** de los documentos que aún permanezcan en el sistema, incluidos los planes de conversión o de correspondencia de datos (véase el apartado 7.2).

9.6 Almacenamiento y manipulación

Los documentos se deberían almacenar en soportes y formatos que garanticen su **disponibilidad, fiabilidad, autenticidad** y conservación durante el periodo de tiempo que sea necesario (véase el apartado 8.2). Las cuestiones relacionadas con su mantenimiento, manipulación y almacenamiento surgen a lo largo de toda su existencia y no únicamente cuando pasan a ser inactivos.

Los documentos necesitan de unas condiciones de almacenamiento y de unos procesos de manipulación que tengan en cuenta sus propiedades físicas y químicas concretas. Los documentos de valor permanente, independientemente de su formato, requieren un almacenamiento y manipulación de mayor calidad para conservarlos a largo plazo. Las condiciones de almacenamiento y los procesos de manipulación deberían

diseñarse con el objetivo de **proteger los documentos contra el acceso y la destrucción no autorizados**, la pérdida, el robo y las catástrofes.

Las organizaciones deberían aplicar políticas y directrices que permitan la **conversión** o la **migración** de los documentos de un sistema de gestión de documentos a otro.

Los sistemas de gestión de documentos electrónicos se deberían diseñar de modo que los documentos permanezcan **accesibles, auténticos, fiables** y **utilizables** durante todo el periodo de conservación, con independencia de cualquier cambio operado en el sistema; como, por ejemplo, la migración a un software diferente, una nueva presentación en formatos de emulación o cualquier otra forma futura de presentar los documentos. **Cuando uno de estos procesos tiene lugar, se debería conservar un testimonio del mismo** junto con los datos relativos a cualquier variación del diseño y formato de los documentos.

2.3.1.2. ISO/TR 15489-2: Information and documentation – Records management – Part 2: Guidelines.

Los principales puntos de esta norma técnica en materia de conservación de documentos electrónicos a largo plazo son:

4.3.7.3 Almacenamiento digital

El almacenamiento de documentos en formato electrónico requiere planes y estrategias de almacenamiento complementarios para **prevenir posibles pérdidas**.

a) los sistemas de **copias de seguridad** previenen la pérdida de documentos como consecuencia de fallos en el sistema. Dichos sistemas deberían proporcionar acceso habitual y urgente a las copias de seguridad e incluir la realización periódica de copias de seguridad, copias múltiples en diversos soportes y almacenamiento de copias de seguridad en diferentes ubicaciones;

b) para prevenir el daño físico de los soportes puede resultar necesario aplicar procesos de mantenimiento. Puede ser necesario copiar los documentos en **versiones más actuales de los mismos soportes** (o en soportes diferentes) para prevenir el deterioro de los datos; y

c) la **obsolescencia del hardware y el software** utilizado puede afectar a la legibilidad de los documentos electrónicos almacenados. Véase el apartado 4.3.9.2 para mayor información.

4.3.9.2 Conservación permanente

Los documentos que se hayan retirado de los sistemas en funcionamiento deberían ser **accesibles y recuperables** durante todo su periodo de conservación. Las características de los documentos, tal como se exponen en el apartado 7.2 de la Norma ISO 15489-1:2001, deberían mantenerse. En aquellos casos en que los documentos se trasladen del entorno físico inmediato de la unidad productora a otra ubicación física, la responsabilidad para autorizar la destrucción o para tomar otras decisiones de disposición es asumida por la unidad mencionada.

Los documentos que han sido **identificados para su conservación permanente** deberían ser almacenados en un entorno apropiado para su conservación a largo plazo.

Las estrategias de conservación de documentos, especialmente de los documentos electrónicos, pueden elegirse en función de su capacidad para mantener la accesibilidad, integridad y autenticidad de los mismos a lo largo del tiempo, así como de su relación coste-rendimiento.

Las estrategias de conservación pueden incluir la copia, conversión y migración de documentos.

a) La **copia** es la producción de un ejemplar idéntico en el mismo tipo de soporte (papel/microfilm/electrónico), por ejemplo, de papel a papel, de microfilm a microfilm, o la producción de copias de seguridad de documentos electrónicos (que también pueden realizarse en otro tipo de soporte).

b) La **conversión** implica un cambio del formato del documento pero garantiza que este documento mantiene la misma información primaria (contenido). Por ejemplo, la conversión en microfilm de documentos en papel, el escaneado, o el cambio de los juegos de caracteres.

c) La **migración** engloba un conjunto de tareas organizadas concebidas para transferir periódicamente material digital de una configuración de hardware / software a otra, o de una generación tecnológica a otra. El objetivo de la migración consiste en conservar la integridad de los documentos y mantener la capacidad de recuperación, visualización y cualquier otro uso. La migración puede darse cuando el hardware o el software caen en desuso, o bien para trasladar los documentos electrónicos de un formato a otro.

Podrán utilizarse **otros métodos de conservación** de documentos electrónicos durante largos periodos de tiempo **a medida que las nuevas tecnologías estén a nuestra disposición**.

Las estrategias de conservación de los documentos electrónicos y de los metadatos asociados eliminados de los sistemas han de ser formuladas e integradas en todos los procesos de diseño del sistema para garantizar que los documentos y sus metadatos seguirán siendo accesibles y utilizables durante todo el plazo de conservación.

Los documentos pendientes de destrucción pueden ser identificados de manera que se lleve a cabo su **destrucción sistemáticamente, cuando el plazo de conservación haya expirado** (por ejemplo, anualmente).

Quando el almacenamiento de los documentos se confíe a una empresa de servicios o se trasfieran a una autoridad archivística externa, ya sea como resultado de una acción de disposición o por otras razones, se establece un acuerdo formal entre el (los) custodio(s) y la parte transferente, describiendo las obligaciones de conservación de los documentos, las reglas de gestión, y las condiciones de tratamiento y acceso.

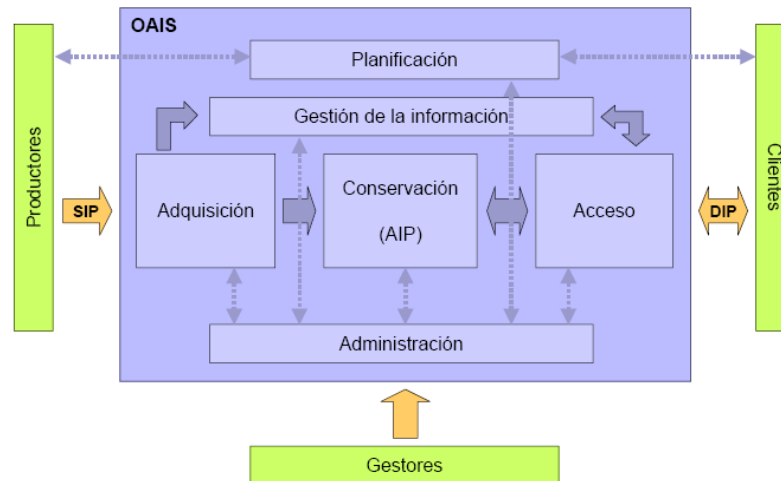
5.3 Valor probatorio

Los gestores de documentos deberían ser conscientes de la magnitud del desafío legal al que se enfrentan al presentar documentos como pruebas en un tribunal de justicia. Si la **integridad** o la **autenticidad** de un documento se pone en duda durante el juicio en razón de alegaciones de falsificación, incompetencia, funcionalidad inadecuada del sistema o fallo del mismo, el valor probatorio o peso evidencial que el tribunal atribuye al documento puede perderse o, al menos, reducirse en detrimento del caso.

Los gestores de documentos deberían contar con pruebas rápidamente disponibles para demostrar y probar el cumplimiento por parte de la organización de la legislación, las políticas y los procedimientos a lo largo de la vida del sistema. También debería ser posible demostrar que el sistema estaba funcionando tal y como estaba previsto de acuerdo con las prácticas habituales de la organización. Los documentos relativos a la **supervisión** y **auditoría** de los procesos del sistema deberían dar evidencia de todo ello.

2.3.1.3. ISO 14721:2003. Space data and information transfer systems – Open archival information system – Reference model.

La norma ISO 14721:2003 (OAIS) define el funcionamiento y las características de un archivo digital a largo plazo.



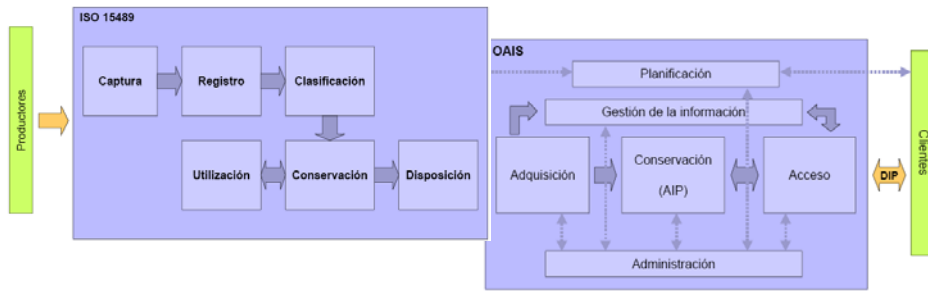
Según Jordi Serra en “La firma electrónica y el archivo digital”;

“El Reference model for an open archival information system (OAIS) ofrece el marco para definir un sistema de archivo digital orientado a la conservación a largo plazo, proporcionando la conceptualización y la terminología para establecer los elementos, las fases y el funcionamiento de este archivo. Un OAIS se define como un conjunto de personas y sistemas que han aceptado la responsabilidad de conservar información y hacerla accesible a una determinada comunidad. El modelo OAIS estructura su funcionamiento en tres etapas:

- **Adquisición** (ingest). Sea a través de un proceso previo de valoración y selección, sea a partir de la adquisición directa, **los documentos se reciben en su formato original**. En esta fase se realiza la transformación de los documentos originales en objetos digitales conservables, lo que implica la verificación de sus requisitos de conservabilidad (validación de la sintaxis, cumplimiento de reglas de integridad en bases de datos, y ausencia de virus, contraseñas y compresiones), **la migración a un formato más estable** y la encapsulación por agrupaciones documentales. A continuación **se completa su descripción**, opcionalmente **se firman**, y se copian al dispositivo de almacenamiento.
- **Conservación** (archival storage). Se lleva a cabo en un repositorio digital seguro, y en el formato de conservación a largo plazo. Periódicamente se aplican los mecanismos necesarios para **chequear los errores y garantizar la legibilidad**. En función de la transformación que estos mecanismos realicen sobre el código del documento original, hablaremos de conservación del entorno tecnológico original cuando no se realice ningún tipo de transformación, de migración cuando se modifique el código fuente del documento, y de emulación cuando se modifique el código del entorno tecnológico del documento. La migración puede realizarse dentro del entorno tecnológico original (compatibilidad retroactiva e interoperabilidad), a un entorno neutro (conversión a estándar), a un entorno predefinido (conversión a formato de emulación) o, simplemente, a otro entorno (cambio de medio o soporte físico).
- **Acceso** (access). La recuperación de los documentos se lleva a cabo en tres etapas. En primer lugar se consulta el inventario o catálogo de documentos, construido a partir de los metadatos. Una vez localizado, el documento se convierte a un formato que facilite su difusión. Finalmente el documento se transfiere a una área donde sea accesible para sus usuarios durante un tiempo determinado.”

2.3.1.4. ISO 15489+ OAIS

Si conectamos estas dos normas (ISO 15489+ OAIS), observaremos que nos permiten definir con precisión un sistema que gestione el ciclo de vida completo de los documentos electrónicos.



2.3.2. Normativa técnica sobre conservación a largo plazo

- ISO/TR 18492
- ISO/PDTR 26102

2.3.2.1. ISO/TR 18492

Introducción

Este informe técnico es una guía para la garantizar el acceso a largo plazo a información basada en documentos electrónicos. Por largo plazo se entiende un periodo mayor que el que se espera para la tecnología que creó la información.

Requisitos

Una estrategia de conservación a largo plazo debería considerar que la información basada en documentos electrónicos permaneciera:

1. Legible (readable)
2. Inteligible (intelligible)
3. Identificable (identifiable)
4. Recuperable (retrievable)
5. Entendible (understandable)
6. Auténtica (authentic)

Riesgos

1. Deterioro físico del soporte
2. Obsolescencia del soporte
3. Alteración de la información en los sistemas de gestión
4. Información almacenada en un entorno ambiental inadecuado
5. Utilización de muchos paquetes de software y formatos de almacenamiento
6. Dependencia de algunos formatos a ciertos paquetes de software
7. Obsolescencia de los sistemas operativos y los aplicaciones software

Acciones

1. Transferencias a soportes más nuevos
2. Transferencia de la información a sistemas de archivo
3. Almacenar la información basada en documentos electrónicos en un entorno ambiental adecuado (similar a cualquier otra información electrónica)
4. Usar soportes WORM⁸ (Write Once Read Many, es decir, escribe una vez y lee cuanto quieras)
5. Disponer la información en formato de sólo lectura

6. Utilizar CRC⁹ (Comprobación de Redundancia Cíclica)
7. Utilizar funciones hash¹⁰ para demostrar que la información no ha sido alterada
8. Utilizar metadatos para describir la información. Para facilitar la interoperabilidad recomienda ISO/TS 23081-1
9. Actualización de las aplicaciones de software
10. Migrar¹¹ la información basada en documentos electrónicos.
 - Tomar en consideración formatos tecnológicamente neutros como: PDF/A-1, XML, TIFF y JPEG.
11. Medidas de seguridad
 - Control del acceso desde los sistemas de gestión
 - Control del acceso físico
 - Protección ante pérdidas

2.3.2.2. ISO/PDTR 26102

A continuación transcribimos las respuestas de Carlota Bustelo (coordinadora del Grupo de trabajo de Records Management del CTN50 (Comité técnico Nacional en Información y Documentación) de AENOR y representante española en el TC46/SC11 Archives/Records Management de ISO) realizadas, a través del foro Arxiforum, sobre la situación actual (Mayo de 2008) de ISO/PDTR 26102:

*“La ISO 26102 no es norma todavía, pues no ha sido aprobada y publicada. En el argot de ISO es en realidad un DTR (borrador de informe técnico). En la última votación llevada a cabo **recibió muy fuertes críticas** de países muy influyentes (Australia, Canadá, Holanda y USA) que han hecho que el actual borrador se encuentre en lo que podríamos denominar “crisis de identidad”. En los próximos meses se tiene que discutir si se sigue o no adelante con este proyecto de informe técnico ISO. Al ser un Informe técnico tiene un proceso más rápido y con necesidad de menos consenso de si es una Norma, y por lo tanto no es posible comprar el borrador, como si pasa con los borradores de Norma.*

La percepción de la delegación española que acabamos de volver de la reunión del SC11 de ISO, es que este informe no prosperará a no ser que se cambie totalmente de orientación y todo eso no es un proceso rápido. Eso no quiere decir que todos los temas relacionados con la preservación de documentos electrónicos no sea una preocupación del SC, al revés son los temas que más propuestas de normalización reciben. Probablemente pronto veamos normas sobre conversión, migración, repositorios digitales, etc.”

En principio se pretendía una especie de aclaración o extensión de la 15489 para los temas de conservación de documentos electrónicos, pero el resultado es un poco pobre. Te doy mi opinión personal, pero seguro que otros miembros del SC1 de AENOR que han tenido acceso al texto pueden aportar más cosas. Para mi el texto es reiterativo con respecto a la 15489 y sólo aporta pequeñas cosas en la enumeración de las posibles tecnologías a utilizar (sin profundizar) y en el desarrollo de algunos aspectos de acceso a documentos electrónicos que la 15489 deja muy en la superficie. Luego, lo malo es que presenta el sistema de preservación (preservation system) de manera que puede ser interpretado como un sistema completamente distinto al de gestión de documentos. Quizás también tiene un cierto sesgo hacia documentos digitalizados más que a nacidos electrónicamente. De todas maneras España votó afirmativamente pero con comentarios en plan más constructivo que los países que votaron en contra con comentarios demoleedores que tachaban el texto de inútil, disperso y por lo tanto sin un sentido claro.

Yo creo que el cambio de orientación debería ser bastante radical para que se convierta en una herramienta útil para una organización que se plantea acometer un programa o proyecto de conservación de documentos electrónicos. Además las otras propuestas de normas que han ido surgiendo van pisándole el terreno o solapándose de manera que se queda un poco sin sentido.”

2.3.3. Normativa sobre formatos de documentos electrónicos

- ISO 19005 (PDF-A)

2.3.3.1. ISO 19005 (PDF-A)¹²

Formato de archivo de documentos electrónicos para conservación a largo plazo.

El estándar PDF/A-1 (ISO 19005-1:2005) se basa en la referencia de formato PDF de nivel 1.4 hecha por Adobe y especifica como usar un subconjunto de componentes PDF para desarrollar programas que creen, reproduzcan y procesen una forma de PDF que sea más adecuada para la preservación de archivos a largo plazo que el simple formato PDF.

Los documentos PDF/A-1 deben incluir

- Fuentes incrustadas
- Color reproducible independientemente
- Metadatos XMP

Los documentos PDF/A-1 no deben incluir

- Encriptamiento
- Compresión LZW
- Ficheros incrustados
- Referencias a contenido externo
- Transparencia PDF
- Multimedia (audio, video)
- Código JavaScript

Actualmente se está trabajando en la versión 2 del estándar ISO 19005 que estará basado en la especificación PDF 1.6 y añade algunas características importantes como son:

- Soporte para compresión de imagen en formato JPEG2000
- Mejor soporte para firma digital
- Soporte para fuentes OpenType
- Gráficos 3D
- Contenido de audio y de video
- Consistencia con otros formatos estándar como PDF/X, PDF/E o PDF/UA

Esta nueva versión del estándar será la 19005-2, es decir, será una extensión de la 19005-1 actual.

Está prevista su publicación para el primer trimestre del año 2009. Posteriormente se avanzará con la creación del formato 19005-3.

2.3.4. Normativa técnica sobre descripción de documentos electrónicos

- ISO 23081
- ISAD
- METS
- PREMIS

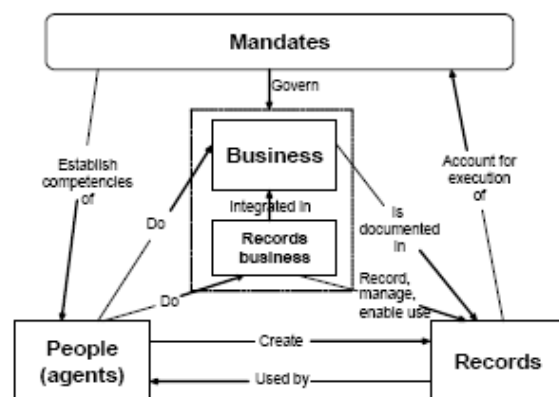
2.3.4.1. ISO 23081

La norma ISO 23081 completa a la norma ISO 15489 en materia de metadatos. Trata sobre los metadatos de gestión de documentos en los procesos de negocio y en la gestión de los documentos. Tiene en cuenta la conservación a lo largo del tiempo.

Los metadatos, además de documentar los procesos de negocio, también documentan los procesos de la propia gestión de documentos, incluyendo cualquier cambio en el contenido, estructura y apariencia.

Entidades sobre las que se asignan metadatos:

- Documentos (records)
- Seguridad
- Acceso
- Regulaciones
- Agentes
- Procesos
- Procesos de gestión de documentos



Metadatos de la norma (se resaltan algunos metadatos de interés especial para la conservación a largo plazo):

- De identificación: Tipo de entidad, Nivel de agrupación, Identificador
- De descripción: Título, Clasificación, Resumen, Lugar, Jurisdicción, Identificadores externos
- De uso: **Entorno técnico**, Derechos, **Acceso**, Usuarios, Idioma, **Integridad**
- **De plan de eventos**: Fecha/Hora, Tipo, Descripción, Relación, Desencadenante
- **De historial de eventos**: Identificador, Fecha/Hora, Tipo, Descripción,
- De relación: Relación, Identificador, Tipo, Fecha

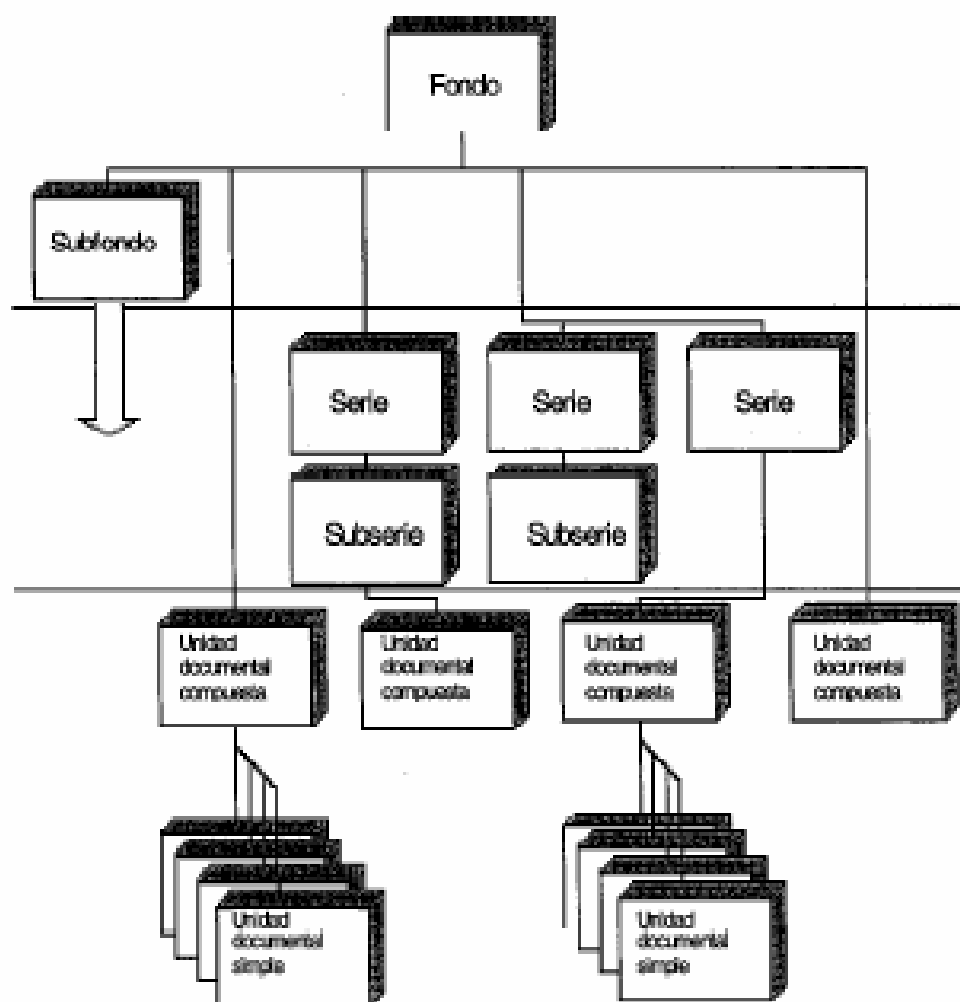
2.3.4.2. ISAD

ISAD es el principal estándar internacional de la descripción archivística. No está orientado específicamente a los documentos electrónicos pero sí a las agrupaciones de orden superior donde se suelen englobar: unidades documentales compuestas, series, fondos documentales.

El Sistema de Gestión de Archivo (SGA) implementa la norma ISAD para la descripción de la información que gestiona.

Resaltamos algunos metadatos de interés para este estudio:

- Valoración, Selección y Eliminación
- Condiciones de acceso
- Características físicas y requisitos técnicos
- Existencia y localización de copias



2.3.4.3. METS: Metadata Encoding & Transmission Standard

El esquema METS¹³ es un estándar para codificar, en lenguaje XML, metadatos descriptivos, administrativos y estructurales de objetos digitales.

Su uso es de utilidad para la conservación de documentos electrónicos a largo plazo por que permite definir características técnicas de los documentos electrónicos y registrar el histórico de las acciones de preservación sobre ellos realizadas.

Está en línea con la especificación OAIS

2.3.4.4. PREMIS¹⁴

Desarrollado por expertos internacionales, incluyendo bibliotecas, museos, archivos, administración pública y sector privado.

Sus objetivos son dos:

- Desarrollar el núcleo para el conjunto de metadatos de conservación, apoyado por un diccionario de datos con una amplia aplicabilidad por la comunidad interesada en este tema.
- Identificar y evaluar estrategias para la codificación, almacenamiento y gestión de metadatos en sistemas de preservación digital

Algunos tipos de metadatos son:

- objectIdentifier (designación unívoca del documento electrónico)
- preservationLevel (tareas de preservación que han de aplicarse)
- objectCharacteristics (características técnicas del documento electrónico)
- fixity (sobre si ha sido alterado de forma no autorizada o no registrada)
- format (formato informático)
- inhibitors (características técnicas del objeto que limitan el uso, acceso o migración)
- creatingApplication (aplicación con la que se creó)
- software (el necesario para acceder)
- hardware (el necesario para acceder)
- relationship (relaciones existentes entre el documento electrónico y otro u otros documentos electrónicos)

2.3.5. Requisitos para los sistemas de gestión de documentos electrónicos de archivo

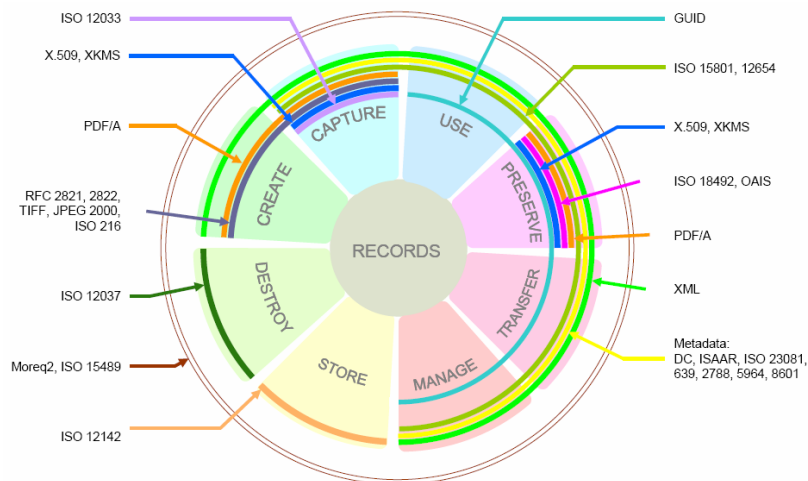
- Moreq
- DoD 5015.2

2.3.5.1. Moreq 2



MoReq 215 actualiza y amplía MoReq 1.

La especificación de requisitos MoReq 2 aporta un modelo gráfico que relaciona los procesos de gestión de archivo de documentos electrónicos de archivo y los estándares internacionales.



Moreq 2 relaciona el proceso de preservación con las siguientes norma técnicas:

- **ISAAR (CPF)** International Standard Archival Authority Record for Corporate Bodies, persons, and Families (International Council on Archives).
- **ISO 639** Codes for the representation of names of languages.
- **ISO 2788** Guidelines for the establishment and development of monolingual thesauri.
- **ISO 5964** Guidelines for the establishment and development of multilingual thesauri.
- **ISO 8601** Representation of dates and times.
- **ISO 14721** Open archival information system – Reference model (OAIS).
- **ISO 15489** Records Management.
- **ISO 15836** The Dublin Core metadata element set.
- **ISO 18492** Long-term preservation of electronic document-based information.
- **ISO 19005-1** Electronic document file format for long-term preservation.
- **ISO 23081** Metadata for records.

- **MoReq2** Update and extension of the Model Requirements for the management of electronic records
- **X.509** ITU-T Recommendation X.509: Open systems interconnection – The Directory: Public-key and attribute certificate frameworks.
- **XKMS** XML Key Management Specification.
- **XML** W3C Extensible Markup Language.

2.3.5.2. DoD 5015.2

El documento equivalente a MoReq en Estados Unidos es **DoD 5015.02-STD: ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS DESIGN CRITERIA STANDARD** ¹⁶ elaborado por el Departamento de defensa.

En materia de conservación de documentos electrónicos a largo plazo dice lo siguiente:

*“C2.2.12.3. **Ability to Read and Process Records.** Since RMAs are prohibited from altering the format of stored records (subparagraph C2.2.3.8.), the organization shall ensure that it has the **ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained.** The organization may meet this requirement by any of the following **means**:*

*C2.2.12.3.1. **Maintaining the hardware and software used to create or capture the record.***

*C2.2.12.3.2. **Maintaining hardware and software capable of viewing the record in its native format.***

*C2.2.12.3.3. **Ensuring backward compatibility when hardware and software is updated.***

*C2.2.12.3.4. **Migrating the record to a new format before the old format becomes obsolete.** Any migration shall be pre-planned and controlled to ensure continued reliability of the record (part 1234.30 of Reference (g)).”*

2.3.6. Normativa técnica sobre firma electrónica

La firma electrónica de los documentos electrónicos debe, a su vez, conservarse para evitar el no repudio de los documentos electrónicos firmados electrónicamente.

La solución de este problema se explica en la “RFC 3126 - Electronic Signature Formats for long term electronic signatures¹⁷” de IETF (Internet Engineering Task Force¹⁸) del 2001, también adoptada en los estándares XAdES (ETSI TS 101 903) y CAdES (ETSI TS 101 733) de ETSI (European Telecommunications Standards Institute¹⁹).

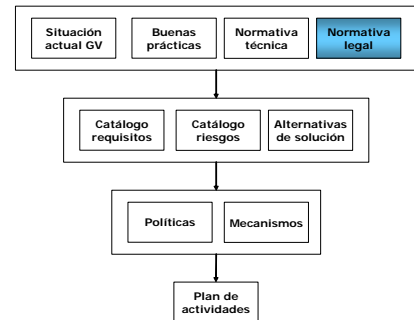
En el anexo 2 se describen los formatos avanzados de firma electrónica.

3 ESTUDIO DE REQUISITOS

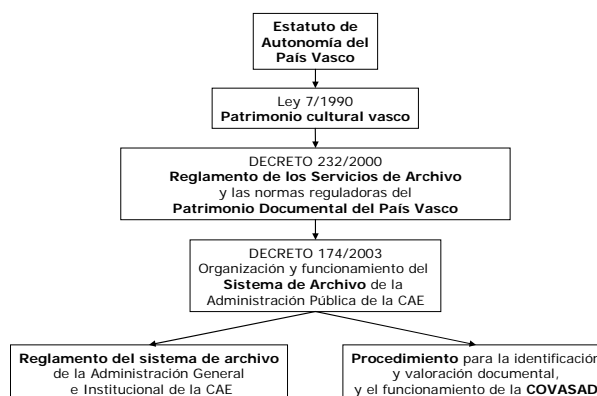
3.1 Normativa legal

La normativa legal que tiene incidencia en la conservación de documentos electrónicos a largo plazo es la siguiente:

- Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del **procedimiento administrativo común**.
- Decreto 232/2000, de 21 de noviembre, por el que se aprueban el **Reglamento de los Servicios de Archivo** y las normas reguladoras del Patrimonio Documental del País Vasco.
- Decreto 174/2003, de 22 de julio, de **organización y funcionamiento del Sistema de Archivo** de la Administración Pública de la Comunidad Autónoma de **Euskadi**.
- Ley 59/2003, de 19 de diciembre, de **firma electrónica**.
- Orden de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del **reglamento del sistema de archivo** de la Administración General e Institucional de la Comunidad Autónoma de **Euskadi**.
- Orden de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, sobre el procedimiento para la identificación y valoración documental, y el funcionamiento de la Comisión de Valoración, Selección y Acceso a la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi (**COVASAD**).
- Ley 11/2007, de 22 de junio, de **acceso electrónico de los ciudadanos a los Servicios Públicos**
- Decreto 232/2007, de 18 de diciembre, por el que se regula la **utilización de medios electrónicos, informáticos y telemáticos** en los procedimientos administrativos



El siguiente diagrama detalla el marco normativo relativo al Archivo:



A continuación se resaltan, para cada normativa legal seleccionada, los artículos que tienen incidencia con la conservación de documentos electrónicos a largo plazo.

3.1.1. Ley 30/1992. Procedimiento administrativo común

Titulo completo:

Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común

Artículo 137. Presunción de inocencia.

3. Los hechos constatados por funcionarios a los que se reconoce la condición de autoridad, y que se formalicen en documento público observando los requisitos legales pertinentes, tendrán valor probatorio sin perjuicio de las pruebas que en defensa de los respectivos derechos o intereses puedan señalar o aportar los propios administrados

Artículo 45. Incorporación de medios técnicos.

5. **Los documentos** emitidos, cualquiera que sea su soporte, por medios **electrónicos**, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, **gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación** y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por éstas u otras Leyes

3.1.2. Decreto 232/2000. Reglamento de los Servicios de Archivo

Titulo completo:

Decreto 232/2000, de 21 de noviembre, por el que se aprueban el Reglamento de los Servicios de Archivo y las normas reguladoras del Patrimonio Documental del País Vasco.

Artículo 6.– Deber de conservación.

1.– Los titulares o poseedores de fondos de archivo, documentos y colecciones de documentos que formen parte del Patrimonio Documental del Pueblo Vasco, están obligados a atender su **conservación y custodia**, a permitir su consulta en los términos previstos en la legislación aplicable, y a facilitar, en su caso, las tareas de inspección por parte de la Administración pública competente, al objeto de velar por el cumplimiento de los deberes previstos en la legislación vigente del Patrimonio Cultural Vasco.

CAPÍTULO II

DE LOS SERVICIOS DE ARCHIVO PÚBLICOS

Artículo 9.– Obligatoriedad de su creación e instalaciones.

3.– El responsable del servicio de archivo elaborará y mantendrá, debidamente actualizado, un **plan de emergencia** que garantice la integridad del Fondo de Archivo **ante posibles desastres** que pudieren poner en peligro su conservación.

Título completo:

Decreto 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi.

Artículo 8.– Departamentos del Gobierno Vasco.

1.– Corresponde a los Departamentos la implantación del Sistema General de Archivo de la Administra

– **Conservar** adecuadamente los documentos generados en el ejercicio de su actividad, durante el período que en cada caso se determine.

Artículo 21.– Responsabilidad de los Archivos de gestión.

La organización y **custodia** de los Archivos de gestión o de oficina estará a cargo del responsable del órgano al que pertenezcan, quien podrá asignar estas funciones a un funcionario de su unidad administrativa cuando el volumen o la intensidad de consulta del archivo lo aconsejen. En la realización de las tareas de gestión el responsable habrá de seguir las directrices e instrucciones emanadas de la Dirección del Sistema.

Artículo 22.– Funciones de los Archivos de gestión o de oficina.

– **Conservar** los documentos generados por la actividad de la propia unidad administrativa durante el período que a tal efecto determine la Dirección del Sistema y, en todo caso, que se señalen en los respectivos Calendarios de Conservación.

– Conservar los documentos en instalaciones adaptadas a la normativa técnica en la materia.

Artículo 24.– Responsabilidad del Archivo General.

La organización y custodia del Archivo General estará a cargo de la Dirección de Recursos Generales del Departamento de Hacienda y Administración Pública, que las ejercerá a través del Servicio correspondiente.

Artículo 25.– Funciones del Archivo General.

– **Custodiar** y organizar los fondos documentales durante los plazos definidos para su permanencia en este archivo.

– **Conservar** los documentos en instalaciones adaptadas a la normativa técnica en la materia.

Artículo 38.– La valoración.

Mediante el proceso de valoración, la Dirección del Sistema apreciará los valores administrativo, histórico, legal, de información y de investigación de los documentos, que servirá de base para establecer los **criterios de conservación** y de eliminación de los mismos, tarea que corresponderá a la Comisión de Valoración, Selección y Acceso de la Documentación.

Artículo 39.– La selección.

Mediante la selección, la Dirección del Sistema determina el destino de los documentos a partir de sus valores, **los plazos de tiempo límites para su conservación** o para su destrucción, los tipos de muestreo aplicables y las modalidades de eliminación.

3.1.4. Ley 59/2003. Firma electrónica.

Titulo completo:

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. La **firma electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
2. La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3. Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
4. **La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.**
5. Se considera **documento electrónico** el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.
6. El documento electrónico será soporte de:
 - a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.
 - b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.
 - c) Documentos privados.
7. **Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.**
8. **El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio.** Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil

Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones públicas.

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Artículo 8. Extinción de la vigencia de los certificados electrónicos

2. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

Artículo 10. Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos

3. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

Artículo 18. Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

Artículo 20. Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.

f) **Conservar** registrada por cualquier medio seguro **toda la información y documentación relativa a un certificado reconocido** y las declaraciones de prácticas de certificación vigentes en cada momento, **al menos durante 15 años** contados desde el momento de su expedición, **de manera que puedan verificarse las firmas efectuadas con el mismo.**

3.1.5. Reglamento del sistema de archivo de la Adm. General de la CAE

Titulo completo:

Orden de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi

Artículo 3.– Definiciones y conceptos básicos.

h) En contraposición a la documentación de archivo, se considera **Documentación de apoyo informativo** a aquellos documentos (impresos, fotocopias de disposiciones normativas, folletos, etc.) cuya utilidad para la Administración radica exclusivamente en su contenido informativo para apoyo de la gestión administrativa, por tanto **no es documentación susceptible** de integración en los expedientes **ni de conservación** en los archivos.

Artículo 5.– **Archivos** de Gestión o **de Oficina** de la Administración General e Institucional.

1.– Los archivos de gestión o de oficina están integrados por la documentación existente en las unidades administrativas en que orgánicamente se estructuran los diferentes Departamentos, Organismos Autónomos, Entes Públicos de Derecho Privado y Sociedades Públicas del Gobierno Vasco, documentación que se corresponde con la etapa inicial o activa del ciclo de vida de los documentos.

2.– Es responsabilidad de los archivos de gestión:

b) La correcta **conservación** de los expedientes completos, de manera que se evite la dispersión y fraccionamiento de la documentación perteneciente a un mismo expediente.

e) La realización de las tareas de **depuración** y **expurgo** o **transferencia** de la documentación teniendo en cuenta los calendarios de conservación definidos para la misma y la normativa relativa a estos procesos.

3.– Como norma general, la documentación permanecerá en estos archivos mientras dure su tramitación administrativa. **Una vez al año se transferirán al siguiente nivel de archivo los expedientes que se hayan concluido**, siguiendo los plazos establecidos en el Calendario de Conservación.

Artículo 7.– El Archivo General.

1.– El Archivo General de la Administración General e Institucional de la Comunidad Autónoma de Euskadi recibe y gestiona la documentación remitida por los archivos de gestión o de oficina y por los archivos centrales de la Administración Institucional, una vez finalizado el plazo de permanencia en estos archivos. Asimismo recibirá la documentación remitida por la Administración del Estado o por las Administraciones Forales en virtud del traspaso de competencias a la Comunidad Autónoma de Euskadi.

2.– Este archivo realiza las siguientes funciones generales en relación a la gestión y tratamiento de la documentación de archivo:

e) La realización del **expurgo** de la documentación en los plazos previstos en el Calendario de Conservación de la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi.

f) La **conservación** y custodia de los fondos documentales existentes durante el plazo de permanencia de la documentación en el Archivo General.

g) La **transferencia al Archivo Histórico** de aquella documentación para la que se establece su conservación permanente.

Artículo 16.– Plan de Infraestructuras y equipamiento.

Periódicamente la Dirección del Sistema de Archivo elaborará un Plan de Infraestructuras y Equipamiento de los archivos del Sistema que contemple:

e) La elaboración de un **programa para la conservación** de los soportes fotográficos, **digitales y electrónicos**.

f) La elaboración de un **Programa de Contingencias** en el que se concreten las **actuaciones** y recursos necesarios **para reaccionar ante las situaciones de riesgo** y emergencias que puedan afectar a la conservación de la documentación.

Artículo 26.– Documentación en otros soportes.

1.– La documentación en soportes distintos del papel se conservará en armarios y contenedores adecuados para su mejor preservación:

c) Los disquetes, CD-ROM, DVD, etc. en ficheros.

2.– Para la conservación de los documentos electrónicos:

a) Se realizarán periódicamente **copias de seguridad** que garanticen la conservación de la información.

b) Se realizarán las **conversiones y o migraciones** que se determinen en el Calendario de Conservación para los documentos de conservación permanente.

3.– Las condiciones específicas para la conservación de la documentación sobre soporte electrónico será objeto de desarrollo en la Norma Técnica que se elabore al efecto.

CAPÍTULO III

TRANSFERENCIAS DE DOCUMENTACIÓN

SECCIÓN PRIMERA

PREPARACIÓN DE LA DOCUMENTACIÓN A TRANSFERIR

Artículo 38.– Actuaciones preparatorias.

Todas las transferencias de documentación entre los distintos niveles de archivo que se realicen en el ámbito del presente Reglamento, se ajustarán al procedimiento aquí definido, realizándose con carácter previo las siguientes tareas:

2.- La documentación que se remita debe ser original o copia única, **depurándose de los expedientes** los duplicados, fotocopias, borradores (sólo en el caso de que éstos no existan se conservará la copia) y **documentación de apoyo informativo**.

3.1.6. Comisión de Valoración, Selección y Acceso a la Documentación (COVASAD).

Titulo completo:

Orden de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, sobre el procedimiento para la identificación y valoración documental, y el funcionamiento de la Comisión de Valoración, Selección y Acceso a la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi (COVASAD).

Nota: Los artículos más relevantes de esta orden ya han sido extraídos en el punto 2.1.3 de este documento

3.1.7. Ley 11/2007. Acceso electrónico a los Servicios Públicos

Titulo completo:

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP)

Artículo 2. Ámbito de aplicación

1. La presente Ley, en los términos expresados en su disposición final primera, será de aplicación:

- a) A las Administraciones Públicas, entendiéndose por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- b) A los ciudadanos en sus relaciones con las Administraciones Públicas.
- c) A las relaciones entre las distintas Administraciones Públicas.

2. La presente Ley no será de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado.

Artículo 6. Derechos de los ciudadanos

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:

- f) A la **conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos** que formen parte de un expediente

Artículo 13. Formas de identificación y autenticación.

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, **sistemas de firma electrónica** que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten **adecuados para garantizar la identificación de los participantes** y, en su caso, **la autenticidad e integridad de los documentos electrónicos**.

2. Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

3. **Las Administraciones Públicas** podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita **identificar la sede electrónica** y el establecimiento con ella de comunicaciones seguras.

b) Sistemas de firma electrónica para la **actuación administrativa automatizada**.

c) Firma electrónica del **personal al servicio** de las Administraciones Públicas.

d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

Artículo 18. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. Para la identificación y la autenticación del ejercicio de la competencia en la **actuación administrativa automatizada**, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

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

Artículo 24. Registros electrónicos.

1. Las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

2. Los registros electrónicos **podrán admitir**:

a) **Documentos electrónicos normalizados** correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

b) **Cualquier solicitud, escrito o comunicación** distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

Artículo 25. Creación y funcionamiento.

3. Los registros electrónicos emitirán automáticamente un recibo consistente en una **copia autenticada** del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

Artículo 30. Copias electrónicas.

1. Las **copias realizadas por medios electrónicos de documentos electrónicos** emitidos por el propio interesado o por las Administraciones Públicas, **manteniéndose o no el formato original**, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, **siempre que el documento electrónico original se encuentre en poder de la Administración**, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

2. Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

4. En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.

5. Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

Artículo 31. Archivo electrónico de documentos.

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares **deberán conservarse** en soportes de esta naturaleza, **ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo**. Se asegurará en todo caso la **posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones**.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la **integridad, autenticidad, confidencialidad, calidad, protección y conservación** de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Artículo 32. Expediente electrónico.

1. El **expediente electrónico** es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

2. El foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda. Este índice garantizará la integridad del

expediente electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

Artículo 34. Criterios para la gestión electrónica.

La aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización de un **análisis de rediseño funcional y simplificación del procedimiento**, proceso o servicio, en el que se considerarán especialmente los siguientes aspectos:

a) La **supresión o reducción de la documentación requerida a los ciudadanos**, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regulación de su aportación al finalizar la tramitación.

3.1.8. Decreto 232/2007, Utilización de medios electrónicos

Título completo:

Decreto 232/2007, de 18 de diciembre, por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos.

Las garantías de **autenticidad, integridad, disponibilidad, confidencialidad y conservación** de la información y de los documentos en que se empleen medios EIT reciben en este Decreto adecuada concreción; se definen los instrumentos que procurarán su cumplimiento y se establecen los mecanismos y técnicas que habrá de utilizar la Administración para su salvaguarda. Se completa este panorama con las correlativas medidas organizativas dirigidas a asegurar la efectividad de tales garantías.

La **firma electrónica reconocida** se erige, con carácter general, tal y como se desarrolla en el capítulo III, en el instrumento que garantizará la **autenticidad e integridad** de las actuaciones, tanto de la Administración como de la ciudadanía.

La **disponibilidad y conservación** se garantizan reconociendo a las personas interesadas la posibilidad de visualizar la información y los documentos electrónicos que formen parte del expediente, así como de descargarlos acompañados de los elementos que permitan acreditar su autenticidad e integridad.

Artículo 2. Ámbito de aplicación

1.– El presente Decreto será de aplicación:

- a) A la Administración General de la Comunidad Autónoma de Euskadi, y a sus Organismos Autónomos.
- b) A los Entes Públicos de Derecho Privado y demás entidades integrantes del sector público de la Comunidad Autónoma de Euskadi, en las actividades que desarrollen con sujeción al derecho público.
- c) A las personas físicas, jurídicas y entes sin personalidad en sus relaciones con las Entidades incluidas en el ámbito de aplicación.
- d) A las relaciones entre la Administración General de la Comunidad Autónoma de Euskadi y las restantes Administraciones Públicas.

2.– Quedan excluidas del ámbito de aplicación de este Decreto y se regirán por su legislación específica:

- a) Las actuaciones y procedimientos propios de los distintos órdenes jurisdiccionales de la Administración de Justicia.

b) La actividad de seguridad de los Cuerpos de Policía dependientes de la Administración de la Comunidad Autónoma de Euskadi.

Artículo 6.– Garantías generales.

La Administración adoptará las medidas dirigidas a garantizar la **autenticidad, integridad, disponibilidad, confidencialidad y conservación** de la información y de los documentos en que se empleen medios electrónicos, informáticos o telemáticos.

Dichas medidas deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los **riesgos** a los que estén expuestos.

Artículo 7.– Garantías de autenticidad e integridad.

1.– La **autenticidad e integridad** de la información y de los documentos en los que se hayan utilizado medios electrónicos, informáticos y telemáticos se garantizarán, con carácter general, por medio de la **firma electrónica reconocida**, en los términos previstos en el capítulo siguiente.

2.– Asimismo, la Administración adoptará las **medidas de seguridad** necesarias para:

a) **prevenir alteraciones o pérdidas** de los datos.

b) **proteger** los sistemas de información y los datos que contienen frente a la interceptación, manipulación y **acceso no autorizados**.

Artículo 8.– Garantías de disponibilidad.

1.– La Administración garantizará a quienes tengan la condición de personas interesadas la posibilidad de visualizar la información y los documentos electrónicos que formen parte del expediente, así como de descargarlos, acompañados, en su caso, de los elementos que permitan acreditar su autenticidad e integridad.

2.– En el caso de **los documentos firmados electrónicamente**, se garantizará la posibilidad de **guardar la firma electrónica, el sellado de tiempo y la constancia de la verificación del certificado electrónico** con el que se hubieran firmado.

4.– **Los documentos electrónicos se pondrán a disposición** de las personas interesadas en formatos que permitan de forma **gratuita la lectura**, comprobación de la firma electrónica y, en su caso, el descifrado.

Artículo 9.– Garantías de confidencialidad.

La Administración garantizará:

a) La **utilización restringida por las personas autorizadas** de los sistemas de información y de los datos que contengan

Artículo 10. Garantías de conservación

2.– **Los documentos firmados electrónicamente podrán conservarse en soportes electrónicos**, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará, en todo caso, la **posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso**.

3.– **Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados**.

Artículo 11.– Sistemas de firma electrónica.

1.– Las personas físicas y jurídicas podrán utilizar la **firma electrónica reconocida** para relacionarse con las entidades incluidas en el ámbito de aplicación de este Decreto. Asimismo, las personas físicas podrán utilizar los sistemas de firma electrónica incorporados al **Documento Nacional de Identidad Electrónico**.

2.– Las entidades incluidas en el ámbito de aplicación de este Decreto podrán utilizar la **firma electrónica reconocida del personal** al servicio de la Administración, de **órgano** administrativo o puesto directivo, y la firma electrónica para la **actuación administrativa automatizada**.

Artículo 13.– Condiciones adicionales a la utilización de la firma electrónica.

1.– Las actuaciones realizadas por medios telemáticos en el ámbito de los procedimientos administrativos, incorporarán, además de la firma electrónica reconocida de la ciudadanía u órgano actuante, el **sellado de tiempo** y la **constancia de la verificación de la vigencia del certificado electrónico** con el que se ha firmado.

Artículo 15.– Generación automatizada de la firma electrónica.

1.– Se entiende por generación automatizada de la firma electrónica aquella que sea resultado de una aplicación informática programada para que opere automáticamente, sin que para su generación se precise la intervención personal y directa de la persona titular del órgano o puesto directivo identificado en el certificado.

2.– La firma electrónica para la actuación automatizada se basará en un certificado electrónico que incluirá el número de identificación fiscal de la Administración o entidad pública e identificará como firmante al órgano administrativo actuante o, en su caso, al puesto directivo que ejerce la competencia. Asimismo, se hará constar en el certificado la identificación de la persona titular del órgano o del puesto directivo.

3.– La firma electrónica automatizada podrá aplicarse en los siguientes supuestos:

a) En actuaciones que consistan en la comunicación o declaración de un hecho, acto o acuerdo preexistente a través del relato o transcripción total o parcial de tales hechos, actos o acuerdos, y

b) En actuaciones que consistan en la constatación de los requisitos previstos en la normativa aplicable y en la posterior declaración, en su caso, de la consecuencia jurídica predeterminada en la misma.

Artículo 35.– Copias electrónicas de documentos electrónicos.

Las copias realizadas por medios electrónicos de documentos electrónicos, manteniéndose o no el formato original, tendrán inmediatamente la consideración de **copias auténticas, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento**.

Artículo 36.– Copia electrónica de documentos originales en papel.

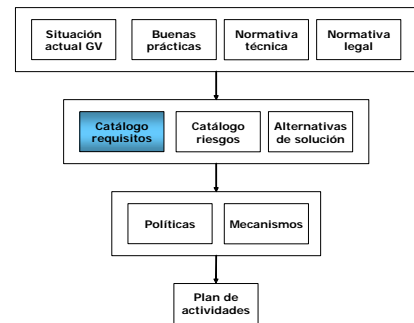
Las copias realizadas por las entidades incluidas en el ámbito de aplicación de este Decreto, utilizando medios electrónicos, de documentos emitidos originalmente por dichas entidades en soporte papel tendrán la consideración de copias auténticas, siempre que se haya comprobado su autenticidad y se añada la firma electrónica del órgano que hubiera emitido el documento original.

3.2 Catálogo de requisitos

En materia de conservación de documentos electrónicos a largo plazo, los principales requisitos a cumplir es garantizar:

- **Autenticidad de los documentos electrónicos**
- **Integridad de los documentos electrónicos**
- **Valor probatorio de los documentos electrónicos (Autenticidad + Integridad)**
- **Disponibilidad de los documentos electrónicos (Accesibilidad + Legibilidad)**
- **Confidencialidad de los documentos electrónicos**

Estas garantías se deben de mantener tanto tiempo como lo determinen los calendarios de conservación.



3.3 Catálogo de riesgos

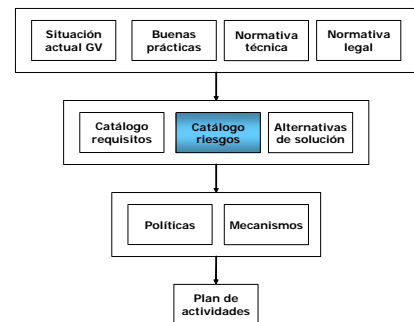
En el proceso de conservación de documentos electrónicos a largo plazo partimos de documentos auténticos e íntegros (de no ser así, este proceso no puede hacer nada por restituir estas características fundamentales) gestionados por sistemas que garantizan su disponibilidad y su confidencialidad.

No hay que conseguir, como en la mayoría de los procesos, un nuevo producto sino lo que hay que hacer es conservar las características con las que ya parte el documento electrónico.

Por tal motivo, es fundamental identificar los riesgos que pueden hacer perder a un documento electrónico sus características.

Los riesgos que podrían hacer perder a los documentos electrónicos su integridad, autenticidad, disponibilidad y/o confidencialidad son:

- Pérdida de la Integridad
 - Alteración del contenido
- Pérdida del valor probatorio (Autenticidad + Integridad)
 - Alteración o borrado de la firma electrónica
 - Obsolescencia del software de verificación de firma
 - Vulneración del sistema de firma electrónica (algoritmos de firma y de hash)
- Pérdida de la Disponibilidad
 - Borrado del documento electrónico
 - Deterioro físico de los soportes en los que se almacenan los documentos electrónicos
 - Obsolescencia del soporte
 - Obsolescencia del formato de documento electrónico
- Pérdida de la Confidencialidad de los documentos electrónicos
 - Acceso no autorizado a la información



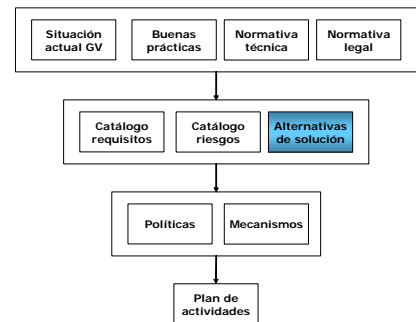
Otros riesgos que pueden dar lugar a alguno o varios de los riesgos identificados en el párrafo anterior son:

- Información almacenada en un entorno ambiental inadecuado
- Utilización de muchos paquetes de software y formatos de almacenamiento
- Dependencia de algunos formatos a ciertos paquetes de software
- Obsolescencia de los sistemas operativos y los aplicaciones software

4 PROPUESTAS DE ALTERNATIVAS DE SOLUCIÓN

El análisis de la normativa legal, las principales normativas técnicas y de las buenas prácticas de otras organizaciones en materia de conservación de documentos electrónicos a largo plazo ha dado lugar a las siguiente relación de operaciones de conservación.

- Transferencia de los documentos electrónicos al Archivo general.
- Copia, en formato PDF/A, de los documentos electrónicos para garantizar su disponibilidad a lo largo del tiempo
- Firma del Archivo general del nuevo documento electrónico con una firma de formato avanzado (CAdeSo XAdES) completándola a modalidad de archivo.
- Chequeo de errores. Control de la integridad mediante CRC u otro mecanismo similar.
- Revisión de la legibilidad
- Copia. Cambio / conversión de formato. Migración..
- Emulación: Consiste en mover los documentos a un nuevo hardware que tiene un software que permite simular el hardware anterior lo cual permite la ejecución del software original. Emulación de los formatos gráficos JPEG y GIF, como mínimo
“La emulación es una técnica sometida aún a muchos interrogantes, de costes imprecisos y, en la fase de conocimiento actual, forzada a un proceso de escalabilidad ad infinitum. De hecho, incluso ha dejado de ser tomada en consideración en ciertas normas técnicas bien consolidadas.”
- Actualización de la firma electrónica. Resecurización del documento electrónico mediante refirma o resellado ante la obsolescencia o vulneración del sistema de firma.
- Describir los documentos electrónicos y los expedientes
 - Datos identificativos y descriptivos (para facilitar la búsqueda) ISO 23081
 - Datos técnicos: formato, versión, etc. (PREMIS y METS)
- Extraer, mediante OCR el texto de los documentos, para facilitar su búsqueda.
- Documentar los procesos de conservación realizados
- Copias de seguridad
 - Realización
 - Restauración en caso de pérdida del documento electrónico o su integridad
- Renovación de los soportes en los que se almacenan los documentos electrónicos
- Supervisiones y auditorías de los procesos del sistema
- Almacenar la información basada en documentos electrónicos en un entorno ambiental adecuado (similar a cualquier otra información electrónica)
- Usar soportes WORM (Write Once Read Many, es decir, escribe una vez y lee cuanto quieras)
- Utilizar funciones hash para demostrar que la información no ha sido alterada
- Actualización de la aplicaciones de software



- Medidas de seguridad
 - Control del acceso desde los sistemas de gestión. Acceso en modo sólo lectura
 - Control del acceso físico
 - Protección ante pérdidas
- Plan de emergencias. Plan de contingencias.
- Realizar los procesos de valoración y selección para establecer los criterios y calendarios de conservación
- Utilizar la firma electrónica reconocida para garantizar la integridad y autenticidad de los documentos electrónicos
- Realizar las transferencias según indican los calendarios de conservación
- Aplicación de los criterios de expurgo
 - Por valoración de la documentación: Expurgar la documentación de apoyo informativo.
 - Por plazos de conservación: Expurgar la documentación según los calendarios de conservación
- Gestión de la obsolescencia de formatos de documentos electrónicos
 - Registro de formatos
 - Seguimiento de la posible obsolescencia
 - Identificación de nuevos formatos
 - Desarrollo de planes de conversión / migración de formatos
 - Conversión / Migración
- Seguimiento de cambios tecnológicos en HW y SW
- Siempre que sea posible, la organización debe generar los documentos electrónicos en el formato de conservación a largo plazo. De esta manera, para estos documentos, no sería necesaria la copia al formato de conservación en largo plazo al transferirlo al Archivo General.
- Fomentar que los documentos electrónicos que reciba la organización sean en:
 - el formato de conservación a largo plazo (PDF/A) o
 - un formato lo más similar posible (por ejemplo, PDF 1.4) o
 - un formato que sea adecuado para la conservación a la largo plazo (por ejemplo, JPG)

5 PROPUESTA DE LA SOLUCIÓN

Este capítulo del estudio enumera las políticas y los mecanismos de conservación de documentos electrónicos a largo plazo.

Estas políticas y mecanismos se han elaborado a partir de:

- los requisitos, los riesgos y las acciones recopilados en este estudio
- la situación actual del Gobierno Vasco.

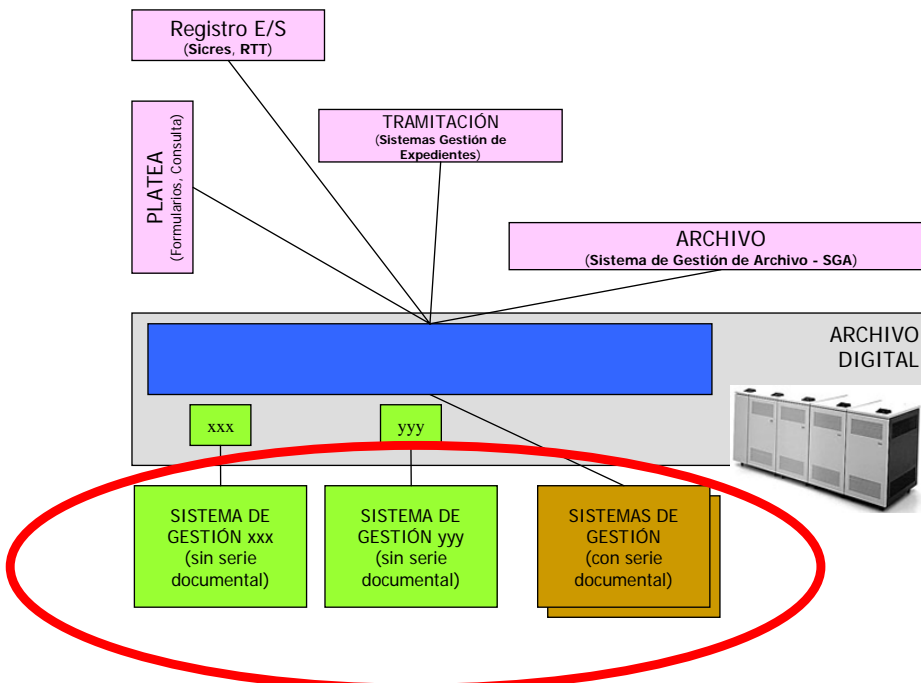
El objetivo final de las políticas y los mecanismos de conservación de documentos electrónicos a largo plazo es garantizar:

- Autenticidad de los documentos electrónicos
- Integridad de los documentos electrónicos
- Valor probatorio de los documentos electrónicos (Autenticidad + Integridad)
- Disponibilidad de los documentos electrónicos (Accesibilidad + Legibilidad)
- Confidencialidad de los documentos electrónicos

Ámbito de las políticas y mecanismos

Según el Modelo de Gestión Documental del Gobierno Vasco “Además de en la tramitación, la gestión documental también está presente en otros procesos del Gobierno Vasco. El Archivo digital también dará servicio a todos los procesos y sus sistemas de gestión.”

El modelo representa esta idea con el siguiente gráfico.



Como ejemplo de este tipo de sistemas de gestión, el Modelo enuncia las siguientes:

- *Infraestructura de Presencia en Internet*
- *Sistemas horizontales de gestión*
 - *Control económico (IKUS)*
 - *Control de personal (GIP)*
- *Sistemas de gestión específicos*
 - *Intranet. Gestión del conocimiento*
- *Sistemas de difusión de información*
 - *Seguimiento de prensa*
 - *Conocimiento jurídico*
 - *Estadísticas*
 - *Publicaciones, BOPV*

Actualmente se están definiendo los requisitos para la gestión de estos documentos electrónicos en el Archivo digital:

- Deben diferenciarse de los documentos electrónicos provenientes de la tramitación.
- Deben tener una estructuración.
- Deben tener unas políticas y calendario de conservación

Los documentos electrónicos que no son fruto de la tramitación (producción administrativa) no están, por ley, sujetos a los requisitos de conservación definidos en este estudio:

- Autenticidad de los documentos electrónicos
- Integridad de los documentos electrónicos
- Valor probatorio de los documentos electrónicos (Autenticidad + Integridad)
- Disponibilidad de los documentos electrónicos (Accesibilidad + Legibilidad)
- Confidencialidad de los documentos electrónicos

No obstante, en algunos casos tendrán, por ejemplo una colección de imágenes de bienes patrimoniales, necesidad de conservar su legibilidad a lo largo del tiempo.

Dar respuesta a esta necesidad parte con una desventaja importante frente a su homóloga para los documentos electrónicos de la producción administrativa. Estos últimos se han definido en un **procedimiento administrativo** donde se explica su uso, se les ha asignado una **serie documental** para su archivo, han sido valorados y seleccionados por el Archivo General y la COVASAD para generar su **calendario de conservación** y, finalmente, son referenciados desde el SGA que controla, entre otros, el proceso de **expurgo**.

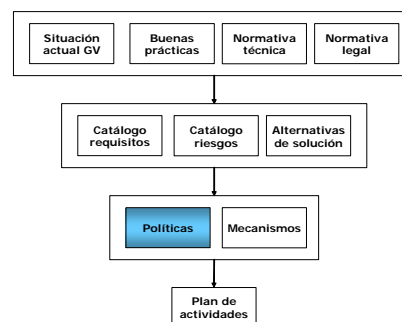
Estas carencias deberán ser solventadas dotando a esta parte del Archivo digital, la de la documentación no administrativa, de un mecanismo de **calendario de conservación sencillo** (ya que no hay que contemplar subsistemas de archivo como en el caso de la producción administrativa) **y genérico** (ya que tiene que ser válido para múltiples fondos documentales) que emule a sus homólogos de la producción administrativa.

Los mecanismos definidos en el presente estudio han de ser igualmente válidos y utilizables para los documentos que no son de la producción administrativa.

5.1 Políticas

Las políticas de conservación a largo plazo de los documentos electrónicos son:

- Relación con el Modelo de Gestión Documental del Gobierno Vasco
- Liderazgo y participación
- La conservación es un proceso dinámico
- Utilizar la firma electrónica reconocida para garantizar la autenticidad e integridad de los documentos electrónicos
- Fomentar el uso de formatos avanzados de firma electrónica
- Ciclo de vida de los documentos
 - elaboración o rediseño de los procedimientos
 - creación
 - uso
 - conservación
 - eliminación
- Herramientas informáticas



A continuación se definen las políticas de conservación a largo plazo de los documentos electrónicos

Relación con el Modelo de Gestión Documental del Gobierno Vasco

La conservación de los documentos electrónicos a largo plazo es un componente del Modelo de Gestión Documental del Gobierno Vasco.

Las políticas y mecanismos enumerados en este documento son un desarrollo del anexo 14 del citado modelo (versión 1.0 de fecha 26.06.2007).

Liderazgo y participación

El liderazgo de la conservación de los documentos electrónicos a largo plazo corresponde al Archivo General tal como lo indica el Reglamento del sistema de archivo de la Administración General de la CAE.

Al archivo general le corresponde la definición, mantenimiento e implantación de las políticas y mecanismos de conservación de documentos electrónicos a largo plazo.

No obstante, esta labor debe realizarse conjuntamente y de manera coordinada con otras unidades/entidades relacionadas, desde distintos ámbitos (normativo, técnico), con la gestión documental: DOMA, DAEAC, DIT, EJIE e Izenpe.

La conservación es un proceso dinámico

La conservación de los documentos electrónicos a largo plazo es un proceso dinámico que requiere de una revisión periódica de las políticas y los mecanismos que lo componen.

Utilizar la firma electrónica reconocida para garantizar la autenticidad e integridad de los documentos electrónicos

Para garantizar la autenticidad e integridad de los documentos electrónicos el Gobierno Vasco debe utilizar (cuando genere documentos electrónicos) o exigir la utilización (cuando reciba documentos electrónicos) de la firma electrónica reconocida tal como se indica en:

- La Ley 59/2003, de 19 de diciembre, de **firma electrónica** dice: “La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.”
- El Decreto 232/2007, de 18 de diciembre, por el que se regula la **utilización de medios electrónicos**, informáticos y telemáticos en los procedimientos administrativos dice: “La autenticidad e integridad de la información y de los documentos en los que se hayan utilizado medios electrónicos, informáticos y telemáticos se garantizarán, con carácter general, por medio de la firma electrónica reconocida”

Fomentar el uso formatos avanzados de firma electrónica (AdES)

Desde el punto de vista legal hay tres tipos de firma:

1. La **firma electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
2. La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3. Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Desde el punto de vista técnico también podemos hacer otras clasificaciones de las firmas electrónicas:

- Formato básico
- Formato avanzado (AdES)
- Formato de archivo (AdES-A)

Formatos de firma desde el punto de vista técnico	Norma técnica: TS 101 733	Norma técnica: TS 101 903	Posibilidad de conservación a largo plazo
Básica	CMS	XML DSig	No
Avanzada	CAdES	XAdES	Puede completarse para ser del tipo Archivo (-A)
Archivo	CAdES -A	XAdES -A	Sí

Los formatos Avanzados de firma electrónica permiten completar ésta al formato Archivo.

El formato Archivo permite la posibilidad de timestamping periódico de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento

Ciclo de vida de los documentos

La conservación de los documentos electrónicos a largo plazo ha de estar presente en todas las fases por las que atraviesa un documento.

- En la **elaboración o rediseño de los procedimientos**:
 - Determinación y difusión de la tipología documental así como su relación con los procedimientos
 - Supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones, o la regulación de su aportación al finalizar la tramitación. (Ver Artículo 34 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos)
 - Realizar los procesos de identificación, valoración y selección de la documentación para establecer los calendarios de conservación y los criterios de acceso.
- En la **creación de un documento electrónico**
 - Por parte de la administración: Siempre que sea posible, el Gobierno Vasco debe generar los documentos electrónicos en el formato de conservación a largo plazo (PDF/A). De esta manera, para estos documentos, no sería necesaria realizar la copia al formato de conservación en largo plazo al transferirlo al Archivo General.
 - Por parte de la ciudadanía: Fomentar que los documentos electrónicos que reciba la organización sean en:
 - el formato de conservación a largo plazo (PDF/A) o
 - un formato lo más similar posible (por ejemplo, PDF 1.4) o
 - un formato que sea adecuado para la conservación a la largo plazo (por ejemplo, JPG)
- En el **uso**
 - Marcar la documentación que es de apoyo informativo, es decir, la que no es de archivo. De esta manera, cuando se transfiera al Archivo general, todos los documentos electrónicos marcados como “de apoyo informativo” serán eliminados.
 - Control del acceso
 - Al cerrar un expediente expurgar todos los documentos que no deban formar parte de él.
- En la **conservación**
 - Realización de las transferencias según los calendarios de conservación
- En la **eliminación**
 - Realización del expurgo según los calendarios de conservación. Realizar el expurgo de la documentación de apoyo informativo

Herramientas informáticas

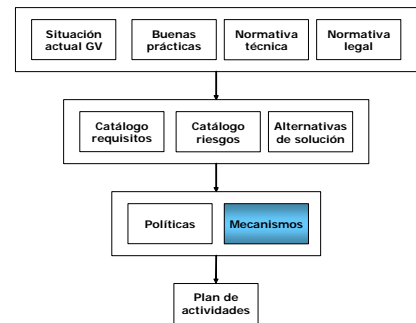
Los mecanismos de conservación de documentos electrónicos a largo plazo se implantarán de manera coordinada en las actuales herramientas informáticas de gestión de archivo:

- El **SGA** quien ya tiene implementado toda la lógica de negocio de la conservación: transferencias, expurgos, calendarios de conservación, etc.
- El **Archivo digital** que almacena el documento y presta servicios documentales.

5.2 Mecanismos

Para una mejor comprensión vamos a agrupar los mecanismos de conservación según las fases principales del modelo OAIS:

- Adquisición de documentos electrónicos
 - Establecer los calendarios de conservación
 - Transferencia de los documentos electrónicos al Archivo general
 - Copia electrónica a un formato de conservación a largo plazo
- Conservación de documentos electrónicos
 - Preventivo
 - Control
 - Mantenimiento
 - Restauración
- Acceso a documentos electrónicos
 - Control de acceso
 - Registros de accesos (LOPD)
 - Disponibilidad



5.2.1. Adquisición de documentos electrónicos

Establecer los calendarios de conservación

La primera de las actividades de la conservación los documentos electrónicos a largo plazo es determinar qué documentos deben conservarse y durante qué plazos de tiempo.

Esta información se recoge en el Calendario General de Conservación que es el fruto de los procesos de identificación, valoración y selección de la documentación.

La correcta selección de los documentos a conservar ahorrará muchos recursos empleados en el resto de mecanismos.

El Calendario General de conservación también detalla el régimen de acceso a la documentación. Esta información es la que define las características de la confidencialidad de los documentos.

Transferencia de los documentos electrónicos al Archivo general

El liderazgo de la conservación de los documentos electrónicos a largo plazo corresponde al Archivo General. Es él quien centraliza e implanta los mecanismos de conservación a largo plazo.

Por lo tanto, cuando los calendarios de conservación de cada serie documental lo indiquen, deben transferirse al Archivo general los expedientes con sus documentos electrónicos.

Copia electrónica a un formato de conservación a largo plazo

Este es el mecanismo principal de la conservación de los documentos electrónicos a largo plazo. Su objetivo es preservar la autenticidad y la integridad de los documentos electrónicos.

Parte de la premisa de que, tarde o temprano, algunos formatos de documentos electrónicos quedarán obsoletos y no podrán visualizarse así como de que los sistemas de firma electrónica son vulnerados con el paso del tiempo.

A continuación recordamos los principales artículos de la normativa legal que permiten este mecanismo.

LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Artículo 30. Copias electrónicas.

1. Las **copias** realizadas por medios electrónicos **de documentos electrónicos** emitidos por el propio interesado o por las Administraciones Públicas, **manteniéndose o no el formato original**, tendrán inmediatamente la **consideración de copias auténticas** con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que **el documento electrónico original se encuentre en poder de la Administración**, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan **comprobar la coincidencia con dicho documento**.

Artículo 31. Archivo electrónico de documentos.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento **o en otro cualquiera** que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la **posibilidad de trasladar los datos a otros formatos y soportes** que garanticen el acceso desde diferentes aplicaciones.

El mecanismo consiste en realizar una copia electrónica en un formato de conservación a largo plazo (PDF/A) a partir del documento original.

Para cada documento electrónico que se transfiera al Archivo general la secuencia de acciones de este mecanismo es la siguiente:

1. Se comprobará si es un documento de apoyo informativo²⁰. En caso afirmativo se borrará y se termina este mecanismo. En caso contrario, se continúa con el mecanismo.
2. Se validará la autenticidad y la integridad del documento electrónico original en el momento de ser transferido al Archivo General
Nota: La realización de esta acción está en discusión entre los integrantes del equipo. Para mí sería ideal poder realizarlo. Actualmente el Archivo general no valida las firmas de los documentos (tanto en papel como electrónicos) que le llegan. El Archivo digital no valida las firmas de los documentos ni dispone de un servicio para ello. Esta validez es responsabilidad de las aplicaciones. Habría que utilizar un servicio universal (que sirva para cualquier tipo de firma) que sea accesible a este mecanismo de conservación.
3. A partir del documento original, se generará una copia electrónica en formato de conservación a largo plazo (PDF/A).

4. El nuevo documento (PDF/A) será firmado por el Archivo general con una firma de formato avanzado (CAAdES o XAdES) completándola a modalidad de archivo (-A).
Nota: Esta modalidad añade la posibilidad de timestamping periódico de documentos archivados para prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento.
5. El nuevo documento y su firma se guardarán en el Archivo digital relacionados con el documento original
Nota: La cuestión clave es si este nuevo documento tiene el mismo valor probatorio que el documento original²¹.
6. Actualizar la descripción técnica (metadatos) de la copia de formato de conservación a largo plazo
7. Documentar la acción de conservación realizada.

A partir de ese momento, cuando se necesite acceder al documento, el Archivo digital pondrá a disposición del solicitante tanto el documento original como su copia en formato de conservación a largo plazo.

Periódicamente, sobre la copia en formato de conservación a largo plazo se realizarán los mecanismos descritos en el presente estudio para garantizar su autenticidad, integridad, disponibilidad y confidencialidad a lo largo del tiempo.

El documento original mantendrá su valor probatorio mientras el formato del documento no quede obsoleto y el sistema de firma no quede obsoleto o se vulnere.

Nota 1: Limitaciones del mecanismo de versiones de conservación a largo plazo.

No todos los formatos de documentos electrónicos se pueden convertir a PDF/A (la versión actual es PDF/A-1). Por ejemplo, los ficheros multimedia no se pueden convertir a PDF/A. En este caso la estrategia debe ser otra y estará en función de los formatos estándares que determine el Gobierno Vasco para esta tipología documental y de las nuevas características del futuro formato PDF/A-2 que si contemplará ficheros multimedia, gráficos 3D,...

El formato PDF/A, por su propia naturaleza, no puede mantener las capacidades de edición de los documentos originales. Por ejemplo

- Las fórmulas de un documento hoja de cálculo se pierden.
- La capacidad de tratar unitariamente los objetos de un documento en formato Power Point se pierde
- La capacidad de modificar un plano dibujado mediante un gráfico vectorial se pierde.

En estos casos, la versión de conservación a largo plazo mantiene el “mensaje” de los documentos originales pero se pierde la capacidad de reutilización.

Nota 2: Conservación del documento original

El documento original, además del valor probatorio del desempeño de las funciones del Gobierno Vasco, tiene el valor de contener una parte del conocimiento de la organización.

Este conocimiento está explicitado en documentos electrónicos cuyo formato, quizás, permita almacenar más información que la versión de conservación a largo plazo.

Para una reutilización del conocimiento albergado en los documentos electrónicos es un valor añadido poner a disposición del usuario el documento original.

5.2.2. Conservación de documentos electrónicos

Los mecanismos de conservación se han agrupado en cuatro tipos

- Preventivo
- Control
- Mantenimiento
- Restauración

A continuación detallamos cada uno de ellos:

- **Mecanismos de conservación preventivos:**
 - Resellado periódico de la firma de las copias en formato de conservación a largo plazo (PDF/A)
 - Actualización periódica de la tecnología (HW y SW) del SGA y del Archivo Digital.
 - Realización de copias de seguridad periódicas
 - Renovación de los soportes en los que se almacenan los documentos electrónicos
 - Gestión de la obsolescencia de formatos de documentos electrónicos
 - Seguimiento de cambios tecnológicos
- **Mecanismos de control de la conservación**
 - Control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital.
 - Revisión de los Registros de accesos²²
- **Mecanismos de mantenimiento de la documentación**
 - Expurgo
 - Transferencia al Archivo histórico
- **Mecanismos de restauración**
 - Restauración de copias de seguridad en caso de pérdida del documento electrónico o su integridad

5.2.2.1. Resellado periódico de las firmas de las copias en formato de conservación a largo plazo (PDF/A)

Las copias en formato de conservación a largo plazo están firmadas por el Archivo general con una firma de formato avanzado (CADES o XAdES) completada a modalidad de archivo (-A)

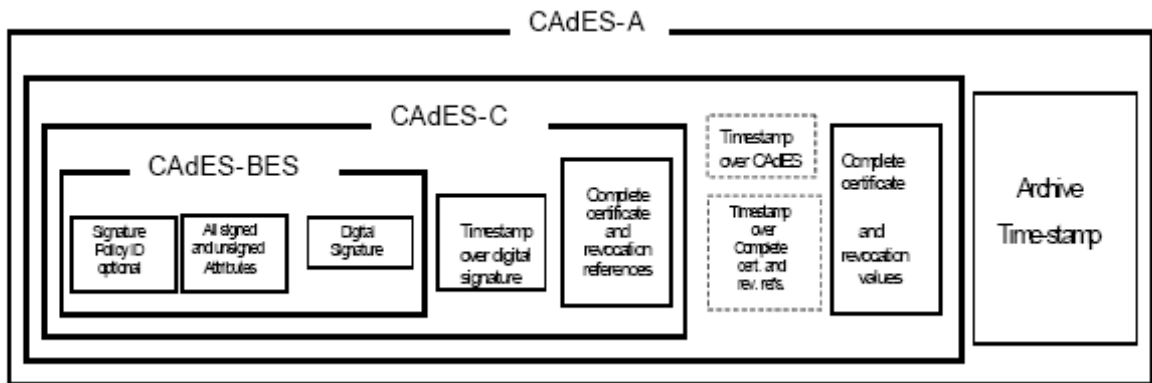
Esta modalidad (-A) incluye toda la información necesaria para su verificación en la propia firma y define cómo mantener la fiabilidad de dicha información mediante sellos de tiempo a lo largo del tiempo. Este perfil de firmas son la base para las firmas electrónicas longevas y a diferencia de otros perfiles, presenta la ventaja de no requerir información adicional custodiada por terceras partes de confianza para poder proceder a su posterior verificación

El objetivo del resellado periódico de las firmas de las copias en formato de conservación a largo plazo es prevenir la pérdida del valor probatorio de dichos documentos electrónicos ante la futura obsolescencia o vulneración del sistema de firma.

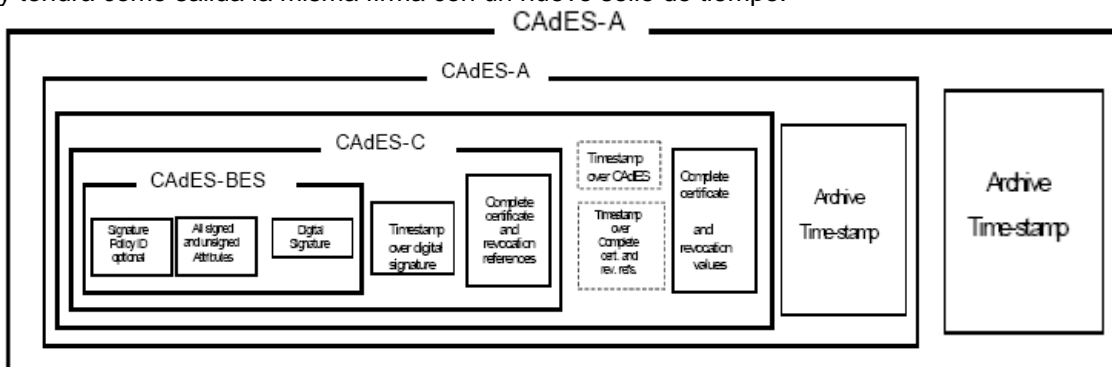
El ámbito y el alcance de actuación del resellado periódico son todos los documentos electrónicos que son copia de los documentos originales.

Los requisitos de este mecanismo son:

- El proceso ha de ser automático.
- La periodicidad de ejecución del proceso debe ser configurable. Será adecuada a las características y tecnología empleada para generar los datos de creación de la firma en formato avanzado. Como orientación inicial, podría ejecutarse cada 4 años.
- El proceso tendrá como entrada una firma de formato avanzado (CADES o XAdES) completada a modalidad de archivo (-A):



y tendrá como salida la misma firma con un nuevo sello de tiempo:



5.2.2.2. Actualización periódica de la tecnología (HW y SW) del SGA y del Archivo Digital

El acceso a los documentos electrónicos se realiza mediante los servicios documentales del Archivo digital.

Esos documentos electrónicos forman parte de unidades documentales (expedientes, proyectos,...) que, pasado un tiempo, estarán archivados en el SGA.

El objetivo de la actualización periódica de la tecnología del SGA y del Archivo Digital es prevenir la pérdida de la disponibilidad de los documentos electrónicos motivada por una pérdida de la operatividad de los citados sistemas.

La responsabilidad de este mecanismo recae en los propios sistemas de gestión: SGA y Archivo Digital.

Ambos sistemas disponen ya de políticas y mecanismos, en línea con las directrices tecnológicas de EJE, que actualizan periódicamente su tecnología.

5.2.2.3. Realización de copias de seguridad periódicas

Los documentos electrónicos se almacenan en Documentum. Documentum asigna a cada documento electrónico un identificador único (OID) Los sistemas de gestión mantienen un enlace con sus documentos electrónicos mediante el identificador (OID) de los mismos.

Copias de seguridad en los sistemas de gestión

Cada sistema de gestión debe realizar sus propias copias de seguridad para no perder los OIDs que enlazan la información de su negocio (expedientes, proyectos, otro tipo de agrupaciones documentales,...) con los documentos electrónicos almacenados en Documentum.

Copias de seguridad en Documentum

El mecanismo de copia de seguridad de documentos electrónicos en Documentum está detallado en el documento "Monitorización y BackUp DCTM" de fecha 28/05/2008.

La información gestionada por los diferentes repositorios del servidor de contenidos consta tanto de **metadatos** almacenados en la **base de datos** como de sus correspondientes **ficheros** de contenido almacenados en las áreas de almacenamiento creadas sobre el servidor de almacenamiento (en este caso, un **sistema de ficheros**).

Por tanto, la realización de la copia de seguridad de la información del servidor de contenidos consistirá en la correspondiente copia de seguridad del usuario ó usuarios (uno por cada repositorio) del servidor de base de datos, mediante las **herramientas propias de dicha base de datos**, así como la del sistema de ficheros, mediante **herramientas propias del sistema operativo o de terceros**.

Así pues, para garantizar la integridad de la información a la hora de una restauración del backup, existen dos posibilidades para la realización de copias de seguridad:

- BackUp "en frío": consiste en aprovechar una ventana horaria en la que el sistema no se utilice (por ejemplo, por la noche), para detener los procesos del servidor de contenidos en el siguiente orden (el arranque de los servicios tras la realización del backup se realizará en orden inverso):
 - Servidor de métodos java: (Documentum Java Method Server)
 - Repositorio(s)
 - Connection Broker(s)
- BackUp "en caliente": si el nivel de servicio requerido no permite detener los procesos del servidor de contenidos, se pueden utilizar herramientas propias del servidor de base de datos para realizar un backup en caliente del usuario asociado a cada repositorio y, para garantizar la integridad de la información a la hora de realizar el backup del servidor de ficheros, habrá que poner el/las área/s de almacenamiento en modo "Read-Only" (desde el cliente web de administración Documentum, Administrador), de modo que los ficheros no puedan ser modificados mientras se realiza dicha copia de seguridad. De este modo, el sistema de ficheros estará accesible en modo consulta. Nota: también puede utilizarse el producto de EMC, Networker (con el módulo "Networker Module for Documentum") para la realización del backup en caliente de Documentum, lo cual permite la posibilidad de recuperación de la información incluso a nivel de objeto del repositorio (por ejemplo, una versión concreta de un documento concreto).

Además de la información de los repositorios, con vistas a recuperar el estado de la instalación del servidor de contenidos, debe realizarse copia de seguridad de ciertos directorios y ficheros de configuración de dicho servidor. En el entorno de producción:

- Export del usuario de BBDD del repositorio de Producción (usuario "dctm" de la instancia "dctm1")
- Áreas de almacenamiento de los repositorios:
 - /datos/dctm (Repositorio de Producción)
- Ficheros de configuración del servidor de contenidos:
 - /opt/dctm/dba/config

5.2.2.4. Renovación de los soportes en los que se almacenan los documentos electrónicos

Los documentos electrónicos están almacenados en soportes físicos que los contienen.

El objetivo de la renovación de los soportes en los que se almacenan los documentos electrónicos es prevenir la pérdida de la disponibilidad de dichos documentos electrónicos.

En este mecanismo hay dos casos de uso

- Soportes de acceso on-line: Son los discos duros de los servidores que almacenan la información del Archivo Digital
- Soportes de acceso off-line: Cintas, disquetes, CDs, DVDs, etc. custodiados por el archivo general u otras unidades.

Soportes de acceso on-line

La renovación de los soportes de acceso on-line del Archivo digital está incluida en los mecanismos de renovación de soportes (discos duros) de EJIÉ.

Soportes de acceso off-line

El Archivo general custodia documentos electrónicos que están en soportes de acceso off-line: Cintas, disquetes, CDs, DVDs, etc.

La renovación de los soportes de acceso off-line presenta las siguientes características

- Es un proceso complejo.
- Es un proceso costoso
- La mayoría de los documentos electrónicos contenidos en dichos soportes no son documentos electrónicos de archivo con obligación legal de conservar. Generalmente son documentación de apoyo informativo o son documentos de archivo duplicados de los originales en soporte papel.
- Una parte de los soportes están dentro de los expedientes. La otra parte está ubicada en ficheros (armarios).

Se propone la creación de dos procedimientos:

- Procedimiento para la migración de los nuevos soportes que ingresen en el Archivo general: Este procedimiento debería ser exhaustivo, tratando cada soporte que sea transferido al Archivo general. La ejecución de este proceso debería empezar desde el cierre del expediente donde se identifiquen los soportes que deben ser conservados y se expurguen los soportes que son de apoyo informativo.
- Procedimiento para la migración de los soportes que actualmente están custodiados por el Archivo general: Este procedimiento debería ser selectivo migrando solamente los soportes que contengan documentos electrónicos que, por criterios de valoración y selección, deban ser conservados.

Actividades comunes a dichos procedimientos son:

- Identificación de los tipos de soportes
- Estimación del tiempo de vida de cada tipo de soporte
- Identificación, en base a criterios de valoración y selección, de los soportes a conservar
- Planificación de las migraciones de soportes
- Ejecución de las migraciones de soportes
- Conversión de formatos de documentos electrónicos

5.2.2.5. Gestión de la obsolescencia de formatos de documentos electrónicos

El objetivo de la gestión de la obsolescencia de los formatos de los documentos electrónicos es prevenir la pérdida de la legibilidad de los documentos electrónicos.

El ámbito y el alcance de este mecanismo son los formatos de documentos electrónicos que almacena el Archivo digital.

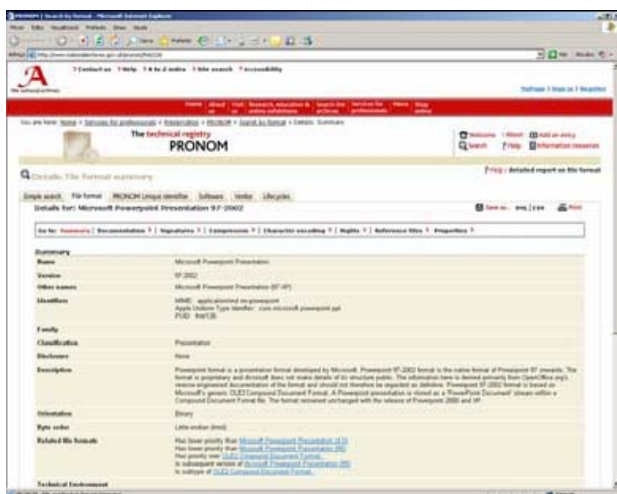
Los mecanismos de conservación están condicionados al formato de los documentos electrónicos. Por ejemplo, algunos se pueden convertir a PDF/A y otros no.

Por lo tanto el mecanismo debe disponer de un registro de formatos de documentos electrónicos que permita seleccionar las acciones de conservación necesarias para cada tipo de formato.

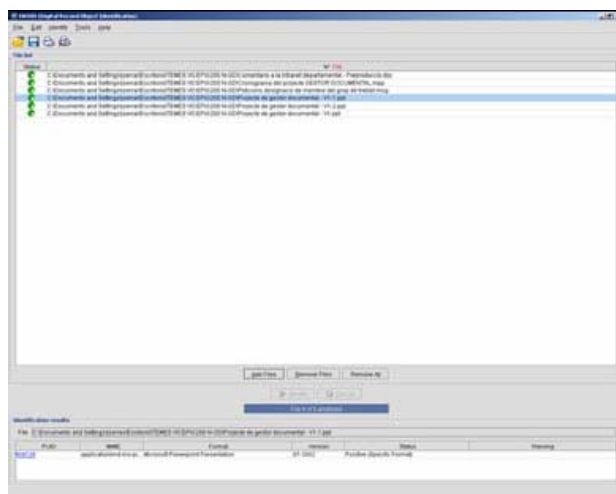
Con este fin se han puesto en marcha varios registros de formatos, y relacionados con ellos se han desarrollado herramientas que permiten la detección automática del formato de un fichero, así como su asociación con la descripción correspondiente proporcionada por el registro.

Uno de los primeros registros de formatos, y el que actualmente ofrece un mayor nivel de servicio, es el registro PRONOM, mantenido por los Archivos Nacionales del Reino Unido. Este registro se puso en marcha en 2004, ofreciendo la consulta en línea del registro de formatos y de software de representación, junto con la posibilidad de exportar la descripción a XML. Posteriormente el registro PRONOM ha desarrollado una herramienta Open Source para la identificación y descripción automática del formato de los ficheros, el Digital Record Object Identification (DROID), que permite a su usuario validar el formato de un conjunto de ficheros y asociarles una descripción normalizada a partir del registro PRONOM.

Registro de formatos PRONOM



Herramienta DROID



Otro registro de formatos de referencia es el Global Digital Format Registry (GDFR), desarrollado por la Harvard University Library. Directamente vinculado al modelo OAIS, se desarrolla según un modelo más próximo al concepto OAIS de red de representación, e incluye una ontología de formatos para la representación de los vínculos entre objetos. Al igual que PRONOM, ha desarrollado una herramienta Open Source para el reconocimiento automático de formatos, el JHOVE - JSTOR/Harvard Object Validation Environment, que a la funcionalidad de identificación añade la validación del cumplimiento de las especificaciones del formato y la caracterización de este formato, es decir la determinación de las propiedades significativas de un fichero u objeto digital cuando está codificado en un determinado formato.

Registro de formatos GDFR



Herramienta JHOVE



5.2.2.6. Seguimiento de cambios tecnológicos

El objetivo del seguimiento de los cambios tecnológicos es detectar:

- Nuevas alternativas tecnológicas en materia de conservación de documentos electrónicos a largo plazo. Por ejemplo, nuevos formatos de firma electrónica.
- Elementos tecnológicos que vayan a quedar obsoletos y pongan en peligro cualquiera de los requisitos (Autenticidad, Integridad, Disponibilidad (Accesibilidad + Legibilidad), Confidencialidad) de conservación de documentos electrónicos a largo plazo.

El ámbito y alcance de este mecanismo son los elementos tecnológicos relacionados con la conservación de los documentos electrónicos a largo plazo:

- Hardware: Soportes y Lectores de almacenamiento
- Software: Sistemas de Gestión de Bases de datos, ECM, Aplicaciones de edición de documentos electrónicos. Visores de documentos electrónicos
- Formatos de documentos electrónicos
- Sistemas y formatos de firma electrónica

El mecanismo debería consistir en la elaboración periódica (semestral, anual) de un informe sobre el estado del arte en materia tecnológica de conservación de documentos electrónicos a largo plazo.

5.2.2.7. Control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital.

El objetivo del control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital es detectar alteraciones o pérdidas de documentos.

Los documentos electrónicos que deben conservarse a largo plazo no deberían, salvo excepciones, ser modificados ni borrados (salvo que sea por un expurgo indicado por el calendario de conservación).

Se propone la utilización del mecanismo de copia de seguridad para implementar este mecanismo, de tal manera que periódicamente se lance una comparación entre una copia de seguridad y el Archivo digital para detectar documentos electrónicos alterados o borrados.

5.2.2.8. Revisión de los Registros de accesos

Tanto el SGA como el Archivo digital actualizan sendos registros de accesos a la información de nivel alto que contienen.

Se entiende por información de nivel alto los:

- a) Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- b) Datos recabados para fines policiales sin consentimiento de las personas afectadas.
- c) Datos derivados de actos de violencia de género.

El objetivo de la revisión de los registros de accesos es

- prevenir la pérdida de la confidencialidad de los documentos electrónicos detectando los intentos no autorizados de acceso
- reparar las carencias de seguridad en caso de detectar accesos no autorizados consumados.

La LOPD impone una serie de requisitos mínimos para los ficheros automatizados con datos de carácter personal de nivel alto: El Reglamento de desarrollo de la LOPD determina que se debe realizar un Registro de accesos:

Artículo 103 – Registro de accesos

- De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
- El período mínimo de conservación de los datos registrados será de dos años.

El Responsable de seguridad es la persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables. Es el encargado de revisar el registro de accesos.

El Responsable del fichero o del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del

tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados

El Responsable de seguridad del SGA y el del Archivo digital **revisarán al menos una vez al mes** la información de control registrada **y elaborará un informe** de las revisiones realizadas y los problemas detectados

Los datos que se pueden obtener del registro de accesos para elaborar el informe podrían ser:

- Todos los accesos ocurridos entre unas fechas concretas, con el detalle de cada evento (usuario que lo realizó, etc.)
- Todos los usuarios que han tenido acceso en un periodo determinado.
- Todos los accesos realizados entre determinadas fechas en un rango de horas.
- Accesos denegados que se han producido en un determinado período de tiempo

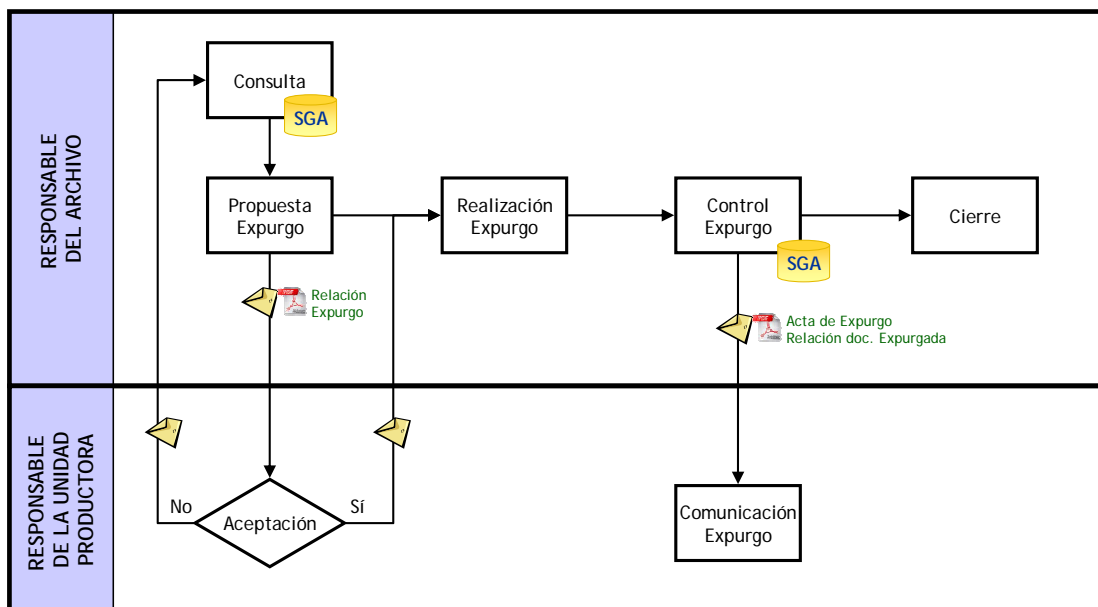
5.2.2.9. Expurgo de documentación

El expurgo de la documentación de archivo, independientemente de que esté en soporte papel o electrónico está automatizado en el SGA.

El SGA automatiza, bajo la supervisión del responsable del archivo, la realización del proceso de expurgo mediante la selección de las series documentales susceptibles de expurgo detectadas por el Sistema en base al calendario de conservación definido.

El Sistema facilita el control del proceso realizado mediante la generación de los correspondientes instrumentos de control (notificaciones, acta de expurgo y relaciones de documentación expurgada) y el seguimiento de la trazabilidad de la documentación objeto de expurgo.

El siguiente diagrama detalla los pasos del proceso de expurgo.



La ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi detalla los siguientes aspectos relativos al expurgo

- Definición
- Responsabilidades
- Procedimiento

Definición

Artículo 3.– Definiciones y conceptos básicos.

l) Se entiende por Expurgo de la documentación el proceso de eliminación o borrado de documentos por cualquier medio que impida su reconstrucción y posterior uso.

Responsabilidades

Artículo 5.– Archivos de Gestión o de Oficina de la Administración General e Institucional.

2.– Es responsabilidad de los archivos de gestión:

e) La realización de las tareas de depuración y expurgo o transferencia de la documentación teniendo en cuenta los calendarios de conservación definidos para la misma y la normativa relativa a estos procesos.

Artículo 7.– El Archivo General.

e) La realización del expurgo de la documentación en los plazos previstos en el Calendario de Conservación de la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi.

Procedimiento

CAPÍTULO VI

SELECCIÓN Y EXPURGO DE LA DOCUMENTACIÓN

SECCIÓN PRIMERA

PROCEDIMIENTO DE EXPURGO DE LA OCUMENTACIÓN

Artículo 58.– Decisión de eliminación.

1.– La selección y eliminación de la documentación se llevará a efecto **en cada nivel de archivo** en función de los plazos de permanencia y conservación que se hayan definido para cada serie documental en el **Calendario de Conservación**.

2.– En ningún caso se podrá eliminar aquella documentación que mantenga su valor administrativo y jurídico.

3.– El Archivo General comunicará a las Oficinas Productoras la relación de documentos que van a ser objeto de expurgo (anexo V).

Artículo 59.– Criterios de destrucción física.

1.– La destrucción física de los documentos se realizará en base a los criterios y plazos definidos en los calendarios de conservación.

2.– Los criterios y el procedimiento establecido para la eliminación de los documentos serán **aplicables a los documentos en cualquier soporte**. El sistema de destrucción será el más adecuado para cada tipo de soporte.

Artículo 60.– Procedimiento de destrucción.

Para la destrucción de la documentación se procederá del siguiente modo:

- a) Determinación de la serie y años a destruir y cajas en las que se contienen la documentación.
- b) Selección de la muestra establecida.
- c) Comunicación a la unidad administrativa productora de la documentación.
- d) Transporte de la documentación al lugar de la destrucción.
- e) Ejecución de la destrucción.
- f) Levantamiento del Acta de Expurgo.
- g) Registro del expurgo realizado.
- h) Remisión de copia del acta de expurgo y de la Relación de Documentación expurgada a la unidad administrativa productora de la documentación.

SECCIÓN SEGUNDA

FORMALIZACIÓN DEL EXPURGO DE LA DOCUMENTACIÓN

Artículo 61.– Documentación relativa al expurgo.

1.– Todo expurgo de documentación deberá estar documentado mediante su correspondiente Acta de Expurgo (anexo VI), en la que se relacionará la documentación eliminada.

2.– Este impreso se realizará por duplicado, conservándose un ejemplar en la unidad administrativa productora de la documentación y el otro en el Archivo General, quien será el encargado de inscribirlo en el Registro de Expurgos de Documentación (anexo VII).

SECCIÓN TERCERA

DESTRUCCIÓN DE LA DOCUMENTACIÓN

Artículo 62.– Contenedores de documentación.

1.– La documentación a eliminar deberá introducirse en contenedores que deberán estar perfectamente cerrados hasta el momento de su destrucción.

2.– Los contenedores de la documentación a eliminar se conservarán de manera ordenada en lugares o locales de acceso controlado, evitando toda posibilidad de apropiación y/o utilización por personas no autorizadas.

Artículo 63.– Control del proceso de destrucción.

Todas las operaciones de selección e instalación de la documentación a destruir en contenedores, transporte al lugar de destrucción y eliminación física de la documentación deberán realizarse de manera controlada y por personal identificado y autorizado para ello.

Artículo 64.– Garantía de la destrucción.

La destrucción de la documentación, cualquiera que sea su soporte, garantizará la imposibilidad de reconstrucción de los documentos o la recuperación de la información en ellos contenida.

SECCIÓN CUARTA

MUESTREO DE DOCUMENTACIÓN A EXPURGAR

Artículo 65.– Selección y conservación de muestras.

1.– De la documentación a expurgar se realizará una selección de documentación a conservar como muestra representativa de la actividad administrativa reflejada por la documentación que se elimina.

2.– La documentación resultante del muestreo realizado se remitirá al Archivo General, siguiendo el procedimiento de transferencias de documentación.

Artículo 66.– Criterios de muestreo.

Tanto la técnica de muestreo y como el volumen de documentación a retener en concepto de muestra se establecerán en el Calendario de Conservación de la documentación generada por la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

5.2.2.10. *Transferencia al Archivo histórico*

La responsabilidad del Archivo General de conservar los documentos electrónicos a largo plazo termina cuando, según el calendario de conservación, hay que expurgar los documentos electrónicos o transferirlos al Archivo Histórico.

De acuerdo con la Disposición Transitoria Primera del Decreto 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi, hasta la entrada en funcionamiento del Archivo Histórico del Gobierno Vasco, toda la documentación que tenga la consideración de histórica, en los términos previstos en la Ley 7/1990, de Patrimonio Cultural, y se haya generado en el ámbito de actuaciones de la Administración General e Institucional de la Comunidad Autónoma de Euskadi será gestionada, organizada y custodiada por el Sistema de Archivo de la misma.

El citado Archivo Histórico del Gobierno Vasco se ha renombrado como el Archivo Histórico Nacional de Euskadi (AHNE)

ARCHIVO HISTORICO NACIONAL DE EUSKADI (AHNE)

Ubicado en el centro de Bilbao, el AHNE se constituirá en el vértice del Sistema Nacional de Archivos además de en la referencia de la conservación de la memoria documental del País Vasco, con una dedicación muy especial a la gestión de la memoria digital²³.

Tal como amplía la nota de prensa²⁴ sobre futura ubicación del Archivo Histórico Nacional de Euskadi en Bilbao (31.03.2006) *“La misión del Archivo Histórico será guardar y difundir la memoria de nuestro país y en este sentido, dará continuidad a la labor de IRARGI, Centro de Patrimonio Documental de Euskadi. Las tecnologías tendrán un papel fundamental en el tratamiento de los documentos y fondos documentales y en el servicio a la ciudadanía”*

El AHNE estará en funcionamiento en el año 2009²⁵.

5.2.2.11. Restauración de copias de seguridad en caso de pérdida del documento electrónico o su integridad

El mecanismo de restauración de copias de seguridad de documentos electrónicos en Documentum está detallado en el documento "Monitorización y BackUp DCTM" de fecha 28/05/2008.

Los pasos a seguir en caso de ser necesaria la restauración de un repositorio de información serían los siguientes:

1. Parar el repositorio y la instancia de base de datos.
2. Restaurar la base de datos mediante las herramientas propias de ésta.
3. Restaurar las áreas de almacenamiento utilizando herramientas propias del sistema operativo o de terceros.
4. Iniciar la instancia de base de datos.
5. Iniciar el repositorio.

Nota: en el caso de que sea necesaria la reinstalación del software del servidor de contenidos, deberá copiarse además el fichero de configuración server.ini del directorio del que se hizo copia de seguridad (ver apartado 3.1), \$DOCUMENTUM/dba/config/<nombre_del_repositorio>.

5.2.3. Acceso de documentos electrónicos

Control de acceso a los documentos electrónicos

Un correcto control de acceso colabora en garantizar la autenticidad, integridad y la confidencialidad de los documentos electrónicos archivados.

- SGA
 - El acceso a los documentos electrónicos que están archivados en el SGA se realiza mediante un control que asigna un rol al usuario en base a la unidad administrativa productiva a la que pertenece el usuario y el tipo de acceso de la serie documental a la que quiere acceder (libre, restringido o confidencial).
- Archivo digital
 - Los usuarios del Archivo Digital se gestionan a nivel de aplicación, es decir, cada aplicación que se integre con el Archivo Digital tendrá un usuario que se corresponderá con su código de aplicación (por ejemplo N61, S54B). La gestión de usuarios nominales se realizará en XLNETs, que es el sistema de seguridad del Gobierno Vasco. Son cada una de las aplicaciones las responsables de gestionar la seguridad a nivel de usuario ya que el Archivo Digital gestionará únicamente el acceso a nivel de aplicación.

Actualización de los Registros de accesos (LOPD)

El SGA y el Archivo digital registrarán todo intento de acceso a información de nivel alto.

Esta información será revisada en el mecanismo Revisión de los Registros de accesos

Mantenimiento de la Disponibilidad

Cuando se necesite consultar un documento electrónico, el Archivo General pondrá a disposición del solicitante tanto el documento original como su copia en formato de conservación a largo plazo.

El Archivo general garantizará de por vida la legibilidad de los documentos en formato de conservación a largo plazo. Actualmente con un visor de PDF sería suficiente.

5.3 **Ámbito de los mecanismos**

La siguiente lista enumera todos los mecanismos:

1. Establecer los calendarios de conservación
2. Transferencia de los documentos electrónicos al Archivo general
3. Copia electrónica a un formato de conservación a largo plazo
4. Resellado periódico de las firmas de las copias en formato de conservación a largo plazo (PDF/A)
5. Actualización periódica de la tecnología (HW y SW) del SGA y del Archivo Digital
6. Realización de copias de seguridad periódicas
7. Renovación de los soportes en los que se almacenan los documentos electrónicos
8. Gestión de la obsolescencia de formatos de documentos electrónicos
9. Seguimiento de cambios tecnológicos
10. Control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital
11. Revisión de los Registros de accesos
12. Expurgo de documentación
13. Transferencia al Archivo histórico
14. Restauración de copias de seguridad en caso de pérdida del documento electrónico o su integridad
15. Control de acceso a los documentos electrónicos
16. Actualización de los Registros de accesos (LOPD)
17. Mantenimiento de la Disponibilidad

Estos mecanismos tienen incidencia en uno o varios ámbitos:

- Archivo de oficina (durante la tramitación)
- Archivo de oficina (tras la tramitación, con el expediente archivado)
- Archivo general
- Archivo histórico
- Documentación no de archivo (toda la documentación que no procede de la tramitación)

La siguiente tabla concreta la incidencia de los mecanismos en cada ámbito.

Mecanismo	Ámbito	AO (Tramitación)	AO (Archivado)	Archivo general	Archivo histórico	Documentación no de archivo
1. Establecer los calendarios de conservación			Según reglamento			Sistema sencillo y genérico
2. Transferencia de los documentos electrónicos al Archivo general			Según calendario de conservación			Según el sistema definido en el mecanismo 1
3. Copia electrónica a un formato de conservación a largo plazo				Al ingresar en el archivo general		A demanda de los SSII
4. Resellado periódico de las firmas de las copias en formato de conservación a largo plazo (PDF/A)				Periódicamente		Periódicamente
5. Actualización periódica de la tecnología (HW y SW) del SGA y del Archivo Digital		Lo realizan los responsables del SGA y el AD en coordinación con EJE				
6. Realización de copias de seguridad periódicas		Lo realiza explotación (EJE)				
7. Renovación de los soportes en los que se almacenan los documentos electrónicos		Identificar los soportes que deben ser conservados y expurgar los soportes que son de apoyo informativo		Migrar los soportes que actualmente están custodiados por el Archivo general		
8. Gestión de la obsolescencia de formatos de documentos electrónicos		Lo realiza el administrador del AD				
9. Seguimiento de cambios tecnológicos		Informe periódico				
10. Control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital		Lo realiza explotación (EJE) e informa al responsable del AD				
11. Revisión de los Registros de accesos		Responsables de seguridad de los SGE		Responsable de seguridad del SGA		Responsables de seguridad de los SSII
12. Expurgo de documentación		Técnicos, según el valor de la documentación	Archiveros, según los calendarios de conservación			Responsables de los SSII, según el sistema definido en el mecanismo 1
13. Transferencia al Archivo histórico				Según calendario de conservación		
14. Restauración de copias de seguridad en caso de pérdida del documento electrónico o su integridad		Lo realiza explotación (EJE)				
15. Control de acceso a los documentos electrónicos		Según la lógica de negocio de los SGE	Control por parte del SGA			Según la lógica de negocio de los SSII
16. Actualización de los Registros de accesos (LOPD)		Lo actualiza cada SGE	Lo actualiza el SGA			Lo actualiza cada SI
17. Mantenimiento de la Disponibilidad				Visor de documento formato de conservación a largo plazo	Visor de documento formato de conservación a largo plazo	Visor de documento formato de conservación a largo plazo

5.4 Cobertura de los requisitos mediante los mecanismos

La siguiente tabla indica para cada mecanismo en requisitos a conservar tiene incidencia.

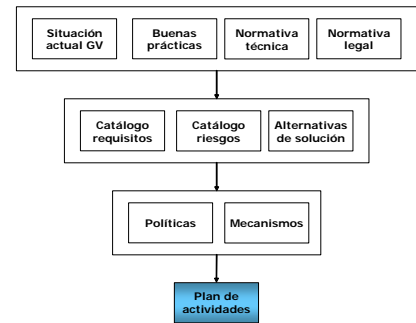
Mecanismo	Requisito	Autenticidad	Integridad	Valor probatorio	Disponibilidad	Confidencialidad
1. Establecer los calendarios de conservación					**	**
2. Transferencia de los documentos electrónicos al Archivo general	*	*	*	*	*	*
3. Copia electrónica a un formato de conservación a largo plazo	**	**	**	**	**	
4. Resellado periódico de las firmas de las copias en formato de conservación a largo plazo (PDF/A)	**	**	**	**		
5. Actualización periódica de la tecnología (HW y SW) del SGA y del Archivo Digital					**	
6. Realización de copias de seguridad periódicas			**	*	**	
7. Renovación de los soportes en los que se almacenan los documentos electrónicos					**	
8. Gestión de la obsolescencia de formatos de documentos electrónicos					**	
9. Seguimiento de cambios tecnológicos	*	*	*	*	*	*
10. Control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital			**	*	**	
11. Revisión de los Registros de accesos					*	**
12. Expurgo de documentación					**	
13. Transferencia al Archivo histórico	*	*	*	*	*	*
14. Restauración de copias de seguridad en caso de pérdida del documento electrónico o su integridad			**	*	**	
15. Control de acceso a los documentos electrónicos	*	*	*	*	*	**
16. Actualización de los Registros de accesos (LOPD)						**
17. Mantenimiento de la Disponibilidad					**	

6 PLAN DE ACTIVIDADES

A continuación enumeramos las actividades para implantar las políticas y mecanismos de conservación de documentos electrónicos a largo plazo.

Se han agrupado en 4 ámbitos:

- Ámbito normativo
- Ámbito de difusión y comunicación
- Ámbito organizativo
- Ámbito técnico



6.1 Ámbito normativo

Las actividades del ámbito normativo son:

- Revisar la validez jurídica, por parte de los servicios jurídicos del Gobierno Vasco, del procedimiento de copia y firma como garante del valor probatorio
- Contraste de las políticas y mecanismos con DOMA, DAEAC, DIT, EJIE e Izenpe
- Aprobación por parte del Archivo General de las políticas y mecanismos
- Adecuación de la normativa existente
 - Modelo de Gestión Documental del Gobierno Vasco
 - Manual de Gestión que recoge la normativa técnica y los procedimientos que afecten a la gestión de los documentos y los archivos del Sistema (según artículo 31 del Reglamento del sistema de archivo de la Adm. General de la CAE)
- Redacción y aprobación del Manual de Seguridad para la elaboración de las aplicaciones informáticas que sirvan de soporte a la tramitación telemática el cual contendrá las medidas de seguridad de carácter general, de índole técnica y organizativa, que aseguren el cumplimiento de las garantías de autenticidad, integridad, confidencialidad, disponibilidad y conservación de la información, de conformidad con los artículos 6 a 10 del DECRETO 232/2007, de 18 de diciembre, por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos.
- Revisión periódica de las políticas y los mecanismos

6.2 Ámbito de difusión y comunicación

Las actividades del ámbito de difusión y comunicación son:

- Difusión interna de las políticas y mecanismos según la planificación del Plan de Comunicación y Difusión del proyecto “Desarrollo y evolución de la plataforma ECM”
- Compartir y contrastar los resultados de este estudio con otras administraciones
- Difusión a la ciudadanía de los formatos preferidos por el Gobierno Vasco para recibir documentos electrónicos.

6.3 **Ámbito organizativo**

Las actividades del ámbito organizativo son:

- Determinación y difusión de la tipología documental así como su relación con los procedimientos.
- Realizar los procesos de identificación, valoración y selección de la documentación para establecer los calendarios de conservación y los criterios de acceso
- Despliegue del SGA en los departamentos del Gobierno Vasco.
- Dotar a los puestos de trabajo de una herramienta que genere documentos en formato de conservación a largo plazo (PDF/A)
- Creación de un observatorio para el seguimiento de cambios tecnológicos en HW y SW
- Estudio de mecanismo de conservación para la documentación no convertible a PDF/A-1: multimedia, gráficos 3D,... Esta información probablemente sí se pueda conservar a largo plazo en el futuro formato PDF/A-2.
- Fomentar el expurgo adecuado de la documentación previo al ingreso en el SGA y la realización de las transferencias según los calendarios de conservación.
- Desarrollo e implantación en el SGA y el Archivo digital de los mecanismos de conservación
- Definir los metadatos técnicos de los documentos electrónicos y de registro de actuaciones de conservación.

6.4 **Ámbito técnico**

Las actividades del ámbito técnico son:

- Implantar y difundir el mecanismo de marcado de la documentación de apoyo informativo
- Implantar en el Archivo general la firma de formato avanzado (XAdES, CAdES)
- Dotar al mecanismo de conservación de un servicio universal de validación de firma electrónica.
- Definir e implantar un proceso de control periódico de la integridad de los documentos electrónicos y firmas almacenados en el Archivo digital.
- Revisión de los Registros de accesos (LOPD)
- Actualización periódica de la tecnología (Oracle, Documentum, etc.) del SGA y del AD.
- Realización de copias de seguridad periódicas
- Renovación de los soportes en los que se almacenan los documentos electrónicos
- Gestión de la obsolescencia de formatos de documentos electrónicos
- Revisión y adecuación del SGA y del Archivo digital a las directrices del Manual de Seguridad

7 ANEXOS

7.1 Normativa jurídica relativa a la facturación electrónica

Esta normativa no es de aplicación al resto de documentos electrónicos pero es en estos momentos el desarrollo normativo más avanzado en materia de conservación de documentos electrónicos a largo plazo.

7.1.1. Facturación telemática y conservación electrónica de facturas

ORDEN EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y **conservación electrónica de facturas**, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación.

Artículo 5. Obligaciones del expedidor en la **conservación de las facturas y documentos sustitutos**.

1. Los empresarios o profesionales **deberán conservar, durante el plazo que resulte de lo dispuesto por la Ley General Tributaria**, los documentos a que se refiere el artículo 19.1 del Reglamento por el que se regulan las obligaciones de facturación.

Esta obligación podrá ser realizada directamente por el propio obligado tributario o por un tercero, actuando este último en nombre y por cuenta del primero, con quien deberá tener el correspondiente acuerdo de prestación de servicios. En cualquier caso, el obligado tributario será el único responsable del cumplimiento de todas las obligaciones que se establecen en el artículo 19.1 del citado Reglamento, debiendo asegurarse de la existencia de las **copias de seguridad** necesarias y de que se apliquen las medidas técnicas y los **planes de contingencias** necesarios que permitan garantizar la **recuperación** de los archivos informáticos **en caso de siniestro** o avería del sistema informático en el que se almacenan las facturas o documentos sustitutos electrónicos.

Artículo 6. Obligaciones de los destinatarios en la **conservación electrónica de las facturas y documentos sustitutos**.

1. Los empresarios o profesionales deberán **conservar, durante el plazo que resulte de lo dispuesto por la Ley General Tributaria**, los documentos a que se refiere el artículo 19.1 del Reglamento por el que se regulan las obligaciones de facturación.

Cuando las facturas o documentos sustitutos se reciban en soporte electrónico, **acompañadas de una firma electrónica reconocida** o de cualquiera otra admitida u homologada por la Agencia Estatal de Administración Tributaria, el destinatario deberá proceder a la **verificación de la firma** y disponer del procedimiento de control interno que a su juicio considere apropiado que le permita **verificar la validez de los certificados utilizados**.

3. La gestión de la conservación de las facturas y documentos sustitutos recibidos debe hacerse ordenadamente, de modo que cualquiera que sea su formato y soporte, y en especial cuando este sea electrónico, **se garantice su legibilidad**, debiendo el obligado tributario facilitar, en su caso, a requerimiento de la Administración tributaria, el descifrado y la decodificación de los datos no auto explicativos.

4. El obligado tributario debe facilitar el acceso completo y sin demora injustificada a las facturas o documentos sustitutivos recibidos, entendiéndose por tal aquél que **permita la consulta** directa de todos y cada uno de ellos, cualquiera que sea su soporte.

Cuando se utilice un sistema informático en la llevanza y conservación de los documentos y, por tanto, éstos tengan un soporte electrónico, tanto en un sistema de almacenamiento local como remoto, el acceso completo debe entenderse como aquél que posibilite una consulta en línea a los datos que permita la visualización de los documentos con todo el detalle de su contenido, la búsqueda selectiva por cualquiera de los datos que deban reflejarse en los libros registro regulados en el artículo 62 y siguientes del Real Decreto 1624/1992, de 29 de diciembre, la copia o descarga en línea en los formatos originales y la impresión a papel de aquellas facturas y documentos sustitutivos que sean necesarios a los efectos de la verificación o documentación de las actuaciones de control fiscal.

Cuando entre las facturas o documentos sustitutivos recibidos existan documentos electrónicos en cuya remisión se optó por la utilización de **firma electrónica** en los términos de los artículos anteriores de esta Orden **como medio para garantizar la autenticidad de su origen e integridad del contenido**, el destinatario **deberá conservar de forma ordenada**, además de las facturas y documentos sustitutivos electrónicos recibidos, **las firmas electrónicas asociadas a cada uno de ellos, cuando no vengán incluidas en el propio fichero que contenga cada documento**. Asimismo, **deberá disponer de los dispositivos de verificación de firma** y de un procedimiento de control interno que garantice de forma adecuada la validez de los certificados electrónicos utilizados por los expedidores, **de modo que se adviertan aquellos que pudieran estar caducados, revocados o suspendidos en el momento de la expedición**.

7.1.2. Expedición de facturas electrónicas a la Administración General del Estado.

ORDEN PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.

... El Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1496/2003, de 28 de noviembre,... **habilita la posibilidad de remisión de las facturas por medios electrónicos**, si bien esta posibilidad se condiciona, por un lado, a que quede **garantizada la autenticidad** del origen y la **integridad** de su contenido y, por otro, al consentimiento del destinatario de la factura prestado de forma expresa.

Artículo 1. Objeto.

Constituye el objeto de la presente orden el establecimiento de unos **estándares y condiciones técnicas** uniformes en la emisión y remisión de facturas que afecten al ámbito subjetivo de la orden, y la regulación de la forma de prestar el consentimiento cuando la Administración sea destinataria de las facturas.

Artículo 2. Ámbito subjetivo.

La presente orden será de aplicación a la **Administración General del Estado** y a los organismos públicos vinculados o dependientes de ella.

Artículo 4. Condiciones técnicas de la remisión de las facturas electrónicas destinadas a, o presentadas ante, la Administración General del Estado o sus organismos públicos vinculados o dependientes.

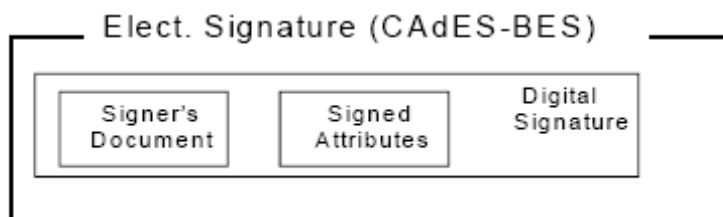
La autenticidad del origen e integridad del contenido de las facturas electrónicas que tengan por destinatario las Administraciones Públicas a las que se aplica la presente orden, en el ámbito de la contratación administrativa, así como la de aquellas que, expedidas entre particulares, se presenten telemáticamente ante tales Administraciones Públicas en el curso de cualquier procedimiento administrativo, **se garantizará mediante la exigencia de firma electrónica avanzada**, en los términos previstos en el artículo 3.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Estas facturas electrónicas deberán hallarse en el formato que se determina en el anexo de esta orden, ajustándose el **formato de firma electrónica** a la especificación XMLAdvanced Electronic Signatures (**XAdES**), ETSI TS 101 903.

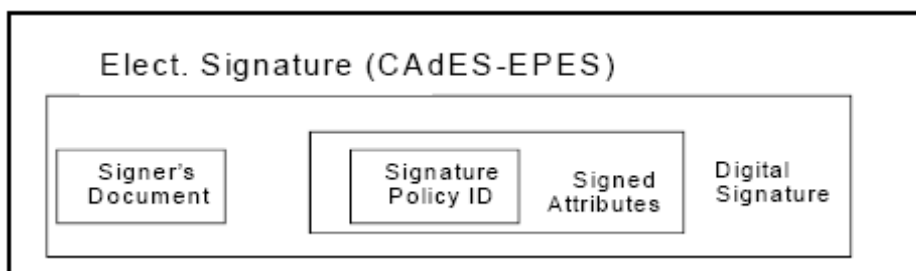
7.2 Formatos de avanzados de firma electrónica

Los estándares XAdES y CADES distinguen cuatro bloques básicos de firma:

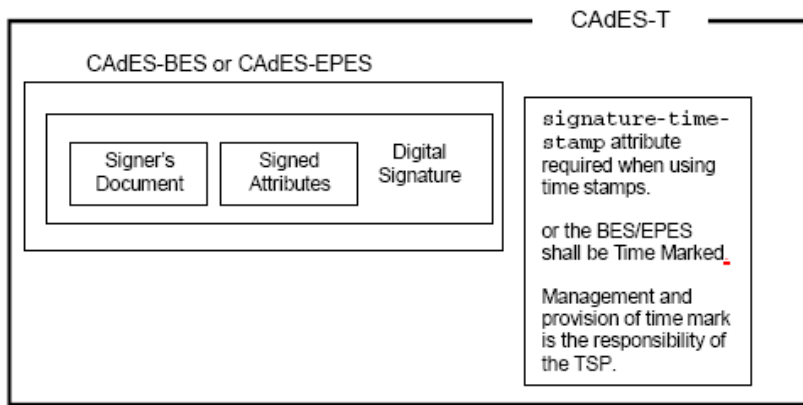
1. **Firma básica (BES)** y firma con política explícita (EPES). La firma no incluye un sello de tiempo, sino que es el firmante quien declara la fecha de firma. Un tercera parte (notaría electrónica) deberá avalar el momento de la firma y la validez de la firma.



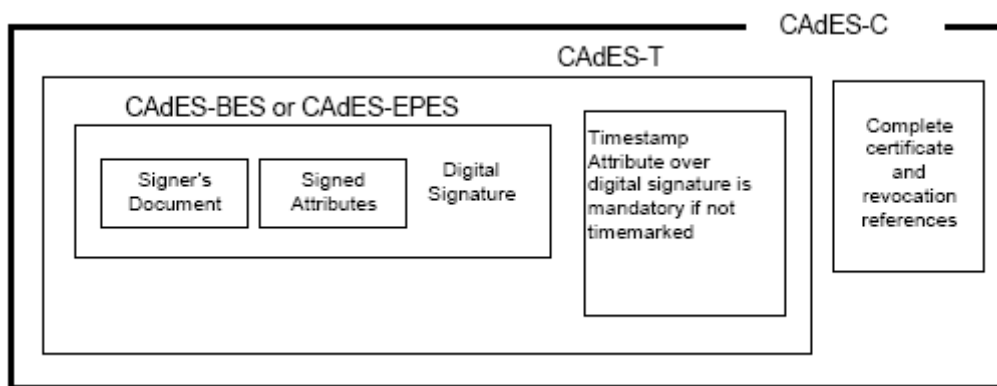
Nota: Esta ilustración y las siguientes están extraídas, a modo de ejemplo, del documento "ETSI TS 101 733 V1.7.3 (2007-01) - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CADES)²⁶"



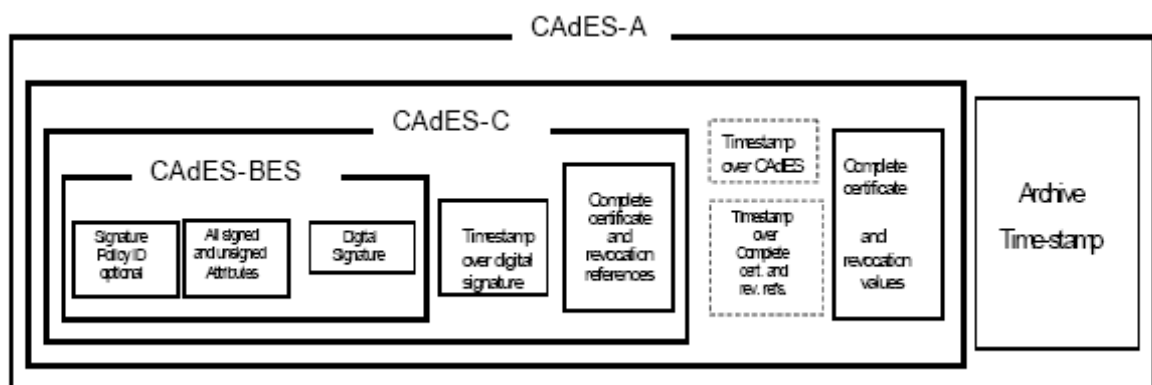
2. **Firma con sello de tiempo (ES-T)**. La fecha de la firma esta avalada por una TSA, por lo que se determina con exactitud si la firma se generó antes de una posible revocación del certificado. No obstante son firmas a las que le faltan evidencias y son de corta duración por lo que se sigue requiriendo una tercera parte (notaría electrónica) que avale la validez de la firma en el momento de su generación.



3. **Firma con información completa de validación (ES-C).** La firma añade un conjunto de referencias a los certificados de la cadena de certificación y su estado (CRL u OCSP), como base para la verificación longeva. Se requerirá que una tercera parte de confianza (por ejemplo, la CA) guarde la información del estado de los certificados.

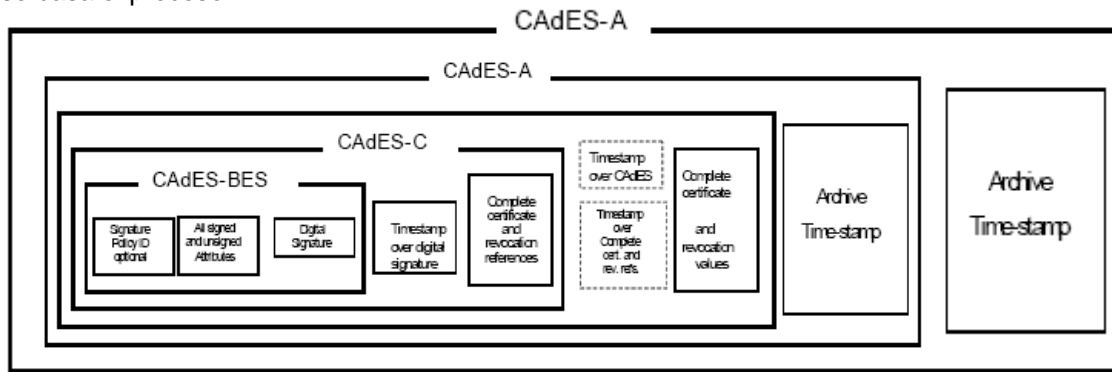


4. **Firma con evidencias electrónicas, o también conocida con la firma de archivo (ES-A).** Incluye toda la información necesaria para su verificación en la propia firma y define cómo mantener la fiabilidad de dicha información mediante sellos de tiempo a lo largo del tiempo.. Este perfil de firmas son la base para las firmas electrónicas longevas y a diferencia de los anteriores perfiles, presenta la ventaja de no requerir información adicional custodiada por terceras partes de confianza para poder proceder a su posterior verificación.



El proceso de time-stamping podría repetirse antes de que sean vulnerables los elementos en los que

se basa el proceso.



XAdes

XAdES sigla en inglés de XML Advanced Electronic Signatures (Firma electrónica avanzada XML) es un conjunto de extensiones a las recomendaciones XML-DSig haciéndolas adecuadas para la firma electrónica avanzada.

XAdES define seis perfiles (formas) según el nivel de protección ofrecido. Cada perfil incluye y extiende al previo:

- **XAdES**, forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada,
- **XAdES-T** (timestamp), añade un campo de **sellado de tiempo para proteger contra el repudio**,
- **XAdES-C** (complete), añade referencias a datos de verificación (certificados y listas de revocación) a los documentos firmados para **permitir verificación y validación off-line en el futuro** (pero no almacena los datos en sí mismos),
- **XAdES-X** (extended), añade sellos de tiempo a las referencias introducidas por XAdES-C **para evitar que pueda verse comprometida en el futuro una cadena de certificados**,
- **XAdES-X-L** (extended long-term), añade los propios certificados y listas de revocación a los documentos firmados para **permitir la verificación en el futuro incluso si las fuentes originales (de consulta de certificados o de las listas de revocación) no estuvieran ya disponibles**,
- **XAdES-A** (archival), añade la posibilidad de timestamping periódico (por ej. cada año) de documentos archivados para **prevenir que puedan ser comprometidos debido a la debilidad de la firma durante un periodo largo de almacenamiento**.

Índice de términos:

Actuación administrativa automatizada	Expediente electrónico
Archivo	Expurgo de la documentación
Archivos federados (Federated Archives)	Fiabilidad
Autenticidad	Firma electrónica
Calendarios de conservación	Firma electrónica avanzada
Certificado	Firma electrónica reconocida
Certificado electrónico	Guardar
Certificado reconocido	Identificación documental
Ciclo de vida de los documentos	Información (Information)
Compulsa	Integridad
Conservar	Interoperabilidad
Conservación (Preservation)	Largo plazo (Long Term)
Conservación a largo plazo (Long Term Preservation)	Legibilidad a largo plazo:
Conversión (Conversion)	Migración (Migration):
Cuadro de Clasificación	Open Archival Information System (OAIS)
Custodia	Paquete de Información de Archivo – PIA (Archival Information Package -AIP)
Custodiar	Preservación
Descripción de los fondos documentales	Prestador de servicios de certificación
Disponibilidad	Proveedor de servicios de certificación
Disposición (Disposition)	Restauración
Documento	Sede electrónica
Documento de archivo	Selección de la documentación
Documentación de apoyo informativo	Sellado de tiempo
Documento electrónico	Soporte
Documento electrónico de archivo	Transformación (Transformation)
Estándar abierto	Valoración documental
Expediente	

Actuación administrativa automatizada

LAECSP

Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

Archivo

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Instancia responsable del tratamiento técnico, difusión y conservación de los fondos documentales.

Archivos federados (Federated Archives)

OAIS – ISO 14721

A group of archives that has agreed to provide access to their holdings via one or more common finding aids.

Autenticidad

ISO 15489

Se debe poder probar que el documento:

- es lo que afirma ser
- ha sido creado por la persona que sea afirma que lo ha creado
- que ha sido creado en el momento que se afirma

FESABID

Que se pueda probar que el documento ha sido creado o enviado por la persona que se afirma que lo ha creado o enviado; y que ha sido creado o enviado en el momento que se afirma.

Calendarios de conservación

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Instrumentos que identifican las series documentales y establecen su permanencia en cada subsistema, su nivel de conservación o eliminación y su accesibilidad.

Certificado

REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.

Es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

DIRECTIVA 1999/93/CE marco comunitario para la firma electrónica

La certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta;

Certificado electrónico

LEY 59/2003, de 19 de diciembre, de firma electrónica.

Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Certificado reconocido

LEY 59/2003, de 19 de diciembre, de firma electrónica.

los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.

Es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12.

DIRECTIVA 1999/93/CE marco comunitario para la firma electrónica

El certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II;

Ciclo de vida de los documentos

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Agrupación de fases por las que atraviesa un documento: creación, mantenimiento, uso y eliminación o conservación definitiva.

Compulsa

Manual de tratamiento de los archivos administrativos (Ministerio de Cultura)

Diligencia que garantiza la fidelidad exacta de la copia con el original que se coteja.

Conservar

RAE

1. Mantener algo o cuidar de su permanencia.
4. Guardar con cuidado algo.

Conservación (Preservation):

UNE-ISO 15489-1 Información y documentación Gestión de documentos Parte 1: Generalidades

Procesos y operaciones realizados para garantizar la permanencia intelectual y técnica de documentos auténticos a lo largo del tiempo.

Manual de tratamiento de los archivos administrativos (Ministerio de Cultura)

Conjunto de procedimientos y medidas destinadas a asegurar, por una parte, la prevención de posibles alteraciones físicas de los documentos y, por otra, la restauración de éstos cuando la alteración se ha producido.

Conservación a largo plazo (Long Term Preservation)

ISO/TR 18492 - Long-term preservation of electronic document-based information

Period of time that electronic document-based information is maintained as accessible and authentic evidence

NOTE: This period of time can range between a few years to hundreds of years, depending upon the needs and requirements of the organization. For some organizations, this period of time would be determined by regulatory compliance, legal requirements and business needs. For other organizations, such as archival repositories holding public records, the period of time required to retain electronic document-based information is usually thought to be hundreds of years.

OAIS – ISO 14721

The act of maintaining information, in a correct and Independently Understandable form, over the Long Term.

Conversión (Conversion)

UNE-ISO 15489-1 Información y documentación Gestión de documentos Parte 1: Generalidades

Proceso de cambiar documentos de un soporte a otro o de un formato a otro.

Cuadro de Clasificación

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Instrumento de gestión que refleja la organización del fondo documental y aporta los datos esenciales de su estructura.

Custodia

Manual de tratamiento de los archivos administrativos (Ministerio de Cultura)

Responsabilidad jurídica que implica por parte de la institución archivística la adecuada conservación de los fondos, cualquiera que sea la titularidad de los mismos.

Custodiar

RAE

1. Guardar con cuidado y vigilancia.

Descripción de los fondos documentales

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Análisis de los documentos de archivo y la elaboración de instrumentos que faciliten el conocimiento y consulta de los fondos documentales.

Disponibilidad

ISO 15489

Documento que puede ser localizado, recuperado, presentado e interpretado

FESABID

Que sea accesible y legible cuando se necesite y a lo largo del tiempo.

MAGERIT

Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información.

ISO 7498-2

Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada.

ITSEC

Prevención de una negación ilícita de acceso a la información o a los recursos.

Disposición (Disposition)

UNE-ISO 15489-1 Información y documentación Gestión de documentos Parte 1: Generalidades

Serie de procesos asociados con la aplicación de decisiones de transferencia, destrucción o conservación de documentos, que se documentan en los calendarios de conservación u otros instrumentos.

Documento

UNE-ISO 15489-1 Información y documentación Gestión de documentos Parte 1: Generalidades

(document) Información u objeto registrado que puede ser tratado como una unidad.

(record) Información creada o recibida, conservada como información y prueba, por una organización o un individuo en el desarrollo de sus actividades o en virtud de sus obligaciones legales.

Nota: El inglés posee tres términos distintos (documents, records y archives), para designar lo que en castellano, como en el resto de lenguas latinas, cuenta con una única voz (documentos). Así, document es el equivalente de documento en su significado genérico, como mera información registrada. Por el contrario, los términos records y archives designan de manera específica a aquellos documentos producidos como prueba y

reflejo de las actividades de la organización que los ha creado, reservándose el empleo de este último a los documentos de carácter histórico.

Por todo ello, la pauta seguida en la traducción es la del empleo del término documento en todos los casos; los posibles problemas de polisemia que pudieran presentarse ocasionalmente, han sido resueltos de la manera usualmente seguida en castellano: mediante la adjetivación o calificación del término allí cuando se pudiera ver como conveniente.

DECISIÓN DE LA COMISIÓN de 7 de julio de 2004 por la que se modifica su Reglamento interno (2004/563/CE, Euratom)

Cualquier documento, tal y como aparece definido tanto en la letra a) del artículo 3 del Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo (1) como en el artículo 1 de las disposiciones relativas a la gestión de documentos anejas al Reglamento interno de la Comisión, en lo sucesivo, «disposiciones relativas a la gestión de documentos»

Documento de archivo

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Toda información registrada, independientemente de su forma y características físicas, recibida, creada o conservada por una institución, entidad o individuo en el desempeño de sus funciones.

Documentación de apoyo informativo

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Aquellos documentos (impresos, fotocopias de disposiciones normativas, folletos, etc.) cuya utilidad para la Administración radica exclusivamente en su contenido informativo para apoyo de la gestión administrativa, por tanto no es documentación susceptible de integración en los expedientes ni de conservación en los archivos.

Documento electrónico

LAECSP

Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

DECISIÓN DE LA COMISIÓN de 7 de julio de 2004 por la que se modifica su Reglamento interno (2004/563/CE, Euratom)

Todo conjunto de datos introducidos o almacenados en cualquier tipo de soporte por un sistema informático o un dispositivo similar, que pueda ser leído o percibido por una persona o por dicho sistema o dispositivo, así como toda visualización y reproducción, en forma impresa o de otro tipo, de tales datos.

LEY 59/2003, de 19 de diciembre, de firma electrónica.

El redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente.

Documento electrónico de archivo

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Todo documento de archivo en soporte electrónico ya sea porque se ha creado mediante una aplicación informática o bien porque se ha digitalizado.

Estándar abierto

LAECSP

Aquel que reúna las siguientes condiciones:

- sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,
- su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Expediente

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

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

Expediente electrónico

LAECSP

Conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

Expurgo de la documentación

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Proceso de eliminación o borrado de documentos por cualquier medio que impida su reconstrucción y posterior uso.

Fiabilidad

FESABID

Que puede ser considerado una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio.

Firma electrónica

LEY 59/2003, de 19 de diciembre, de firma electrónica.

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

REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.

Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

DIRECTIVA 1999/93/CE marco comunitario para la firma electrónica

Los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación.

Firma electrónica avanzada

LEY 59/2003, de 19 de diciembre, de firma electrónica.

La firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.

Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

DIRECTIVA 1999/93/CE marco comunitario para la firma electrónica

La firma electrónica que cumple los requisitos siguientes:

- a) estar vinculada al firmante de manera única;
- b) permitir la identificación del firmante;
- c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;
- d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable;

Firma electrónica reconocida

LEY 59/2003, de 19 de diciembre, de firma electrónica.

La firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Guardar

RAE

1. Tener cuidado de algo, vigilarlo y defenderlo.
5. Conservar o retener algo.

Identificación documental

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Proceso de recopilación de información y estudio de cada una de las series documentales generadas por la Administración.

Información (Information)

OAIS – ISO 14721

Any type of knowledge that can be exchanged. In an exchange, it is represented by data. An example is a string of bits (the data) accompanied by a description of how to interpret a string of bits as numbers representing temperature observations measured in degrees Celsius (the representation information).

Integridad

ISO 15489

Documento completo e inalterado

FESABID

Que no haya podido ser alterado o modificado.

MAGERIT

Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. La integridad está ligada a la fiabilidad funcional del sistema de información, a su eficacia para cumplir las funciones del sistema.

Directrices de la OCDE para una Política Criptográfica

Propiedad de que los datos o la información no hayan sido modificados o alterados de forma no autorizada.

Directrices de la OCDE para la Seguridad de los Sistemas de Información

El hecho de que de los datos o informaciones sean exactos y completos y la preservación de este carácter exacto y completo

ITSEC

Prevención de la modificación no autorizada de información.

ISO 7498-2

Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado

Interoperabilidad

LAECSP

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

Largo plazo (Long Term)

OAIS – ISO 14721

A period of time long enough for there to be concern about the impacts of changing technologies, including support for new media and data formats, and of a changing user community, on the information being held in a repository. This period extends into the indefinite future.

Legibilidad a largo plazo:

DECISIÓN DE LA COMISIÓN de 7 de julio de 2004 por la que se modifica su Reglamento interno (2004/563/CE, Euratom)

El hecho de que la información contenida en los documentos y los metadatos que la acompañan siguen siendo fácilmente legibles, por toda persona que deba o pueda tener acceso a ellos, durante todo el ciclo de vida de dichos documentos, desde su recepción o elaboración formal hasta su transferencia a los archivos históricos de la Comisión y su apertura al público, o hasta su destrucción autorizada en función del período de conservación exigido.

Migración (Migration):

UNE-ISO 15489-1 Información y documentación Gestión de documentos Parte 1: Generalidades

Acción de trasladar documentos de un sistema a otro, manteniendo la autenticidad, la integridad, la fiabilidad y la disponibilidad de los mismos.

ISO/TR 18492 - Long-term preservation of electronic document-based information

process of transferring electronic document-based information from one software/hardware environment or storage medium to another environment or storage medium with little or no alteration of structure and no alteration in content and context

Open Archival Information System (OAIS)

OAIS – ISO 14721

An archive, consisting of an organization of people and systems, that has accepted the responsibility to preserve information and make it available for a Designated Community. It meets a set of responsibilities, as defined in 3.1, that allows an OAIS archive to be distinguished from other uses of the term “archive”. The term “Open” in OAIS is used to imply that this Recommendation and future related Recommendations and standards are developed in open forums, and it does not imply that access to the archive is unrestricted.

Paquete de Información de Archivo – PIA (Archival Information Package -AIP)

OAIS – ISO 14721

An Information Package, consisting of the Content Information and the associated Preservation Description Information (PDI), which is preserved within an OAIS.

Preservación

Manual de tratamiento de los archivos administrativos (Ministerio de Cultura)

Véase Conservación

Prestador de servicios de certificación

REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica.

Es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Proveedor de servicios de certificación

DIRECTIVA 1999/93/CE marco comunitario para la firma electrónica

La entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica;

Restauración

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Proceso técnico que tiene por objeto recuperar la integridad física y funcional de los documentos mediante la corrección del deterioro y los daños sufridos, y la restitución de los documentos a su estado original en la medida en que sea posible, teniendo en cuenta el respeto a la originalidad e integridad del documento y la distinción entre la parte del documento no tratada y la parte restaurada.

Sede electrónica

LAECSP

Dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

Selección de la documentación

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Proceso de determinación de los documentos que van a ser objeto de eliminación o conservación de acuerdo con los plazos que se establezcan en el Calendario de Conservación.

Sellado de tiempo

LAECSP

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

Soporte

Manual de tratamiento de los archivos administrativos (Ministerio de Cultura)

Material físico en el que se registra la información: papel, pergamino, papiro, cintas y discos magnéticos, películas fotográficas, etc.)

Transformación (Transformation)

OAIS – ISO 14721

A Digital Migration in which there is an alteration to the Content Information or PDI of an Archival Information Package. For example, changing ASCII codes to UNICODE in a text document being preserved is a Transformation.

Valoración documental

ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi.

Proceso de análisis y determinación de los valores de los documentos de archivo en función de los efectos que causan y de la información que contienen. Estos valores condicionan la conservación temporal o permanente de la documentación.

7.4 Bibliografía y Referencias

- **La cámara sellada: El gobierno americano construye cámaras acorazadas para conservar los documentos electrónicos**
Luis Hernández Olivera. 2007
- **La gestión de riesgos orientada a la conservación de información en soporte digital**
Bárbara Muñoz de Solano y Palacios. 2006
<http://dialnet.unirioja.es/servlet/articulo?codigo=1986748>
<http://www.ucm.es/BUCM/revistas/inf/02104210/articulos/DCIN0606110125A.PDF>
- **Conservando bits: La conservación de documentos electrónicos**
Raquel Gómez Díaz. 2006
- **Producción y gestión de documentos electrónicos de archivo: Estado de la cuestión en España**
Margarita Vázquez de Parga y Gutiérrez del Arroyo. 2006
- **Los Archivos en la encrucijada: el reto de los documentos electrónicos**
Pedro González García. 2006
- **Acciones de IDA e IDABC en materia de promoción del uso de los formatos abiertos de documentos y de actualización MoReq y los Criterios de conservación**
Miguel Ángel Amutio Gómez. 2006
- **Aspectos económicos del proceso de preservación digital**
Bárbara Muñoz de Solano y Palacios. 2006
<http://dialnet.unirioja.es/servlet/articulo?codigo=2234370>
- **Custodia de larga duración de documentos electrónicos**
Álvaro de la Escalera Armiño. 2006
- **El papel de los metadatos en la preservación digital**
Jorge Candas Romero. Marzo – Abril 2006
<http://eprints.rclis.org/archive/00007682/01/final.pdf>
- **Ponencias de la 2ª Jornada sobre Gestión de Documentos Digitales**
Aedocdigital; directora, María del Valle Palma Villalón. 8 de noviembre de 2006
- **Record keeping in a hybrid environment : managing the creation, use, preservation and disposal of unpublished information objects in context**
Alistair Tough and Michael Moss. 2006
- **La conservación a largo plazo de documentos electrónicos auténticos: hallazgos del Proyecto InterPares**
Luciana Durante. 2005
- **Valoración y selección de documentos electrónicos: principios y aplicaciones**
Jordi Serra Serra. 2005
http://eprints.rclis.org/archive/00005883/01/Jordi_Serra_-_TRIA_12.pdf
- **Todas las normas ISO/UNE en la documentación digital**
Ponencias Jornadas Online, 14 al 19 de julio, 2005 : creación, gestión, seguridad y almacenamiento de los documentos digitales : ISO 15489, ISO 17799, ISO 15801
- **El desarrollo de un programa de preservación ideal para documentos digitales**
Bárbara Muñoz de Solano y Palacios. 2005
<http://www.ucm.es/BUCM/revistas/byd/11321873/articulos/RGID0505220145A.PDF>
- **La gestión de riesgos orientada a la conservación de información en soporte digital**
Bárbara Muñoz de Solano y Palacios. 2005
<http://www.ucm.es/BUCM/revistas/inf/02104210/articulos/DCIN0606110125A.PDF>

- **Documentos electrónicos: manual para archiveros**
Consejo Internacional de Archivos. Comité de archivos de gestión en entorno electrónico. Abril 2005
<http://www.mcu.es/archivos/docs/documentosElectronicos.pdf>
- **Tratamiento digital de imágenes en archivos: modelos de gestión y preservación**
Antonia Salvador Benítez. 2004
- **L'administració electrònica i la gestió de documents**
Jordi Serra Serra. 2003
<http://eprints.rclis.org/archive/00000728/01/BID2003.pdf>
- **Estrategias de conservación de los documentos electrónicos**
Isidro Laso Ballesteros. 2002
- **Estrategias de Preservación de Documentos Electrónicos: el "National Archives And Records Administration" y el "Public Record Office"**
Jordi Serra Serra. 2002
<http://www.ugr.es/~vjarchiv/images/ACTAS%20V%20JORN3.DOC>
- **La administración electrónica y los archivos : amenazas y oportunidades para la archivística**
Jornada Técnica : Toledo, 10 de julio de 2002
- **Los archivos de documentos electrónicos**
Miguel Angel Esteban Navarro. 2001
<http://www.elprofesionaldelainformacion.com/contenidos/2001/diciembre/9.pdf>
http://tramullas.com/jaca/infodigital/contenidos/textos/Esteban_1.pdf
- **Gestión de los documentos digitales: Estrategias para su conservación**
Jordi Serra Serra. 2001
http://eprints.rclis.org/archive/00013259/01/Gesti%C3%B3n_de_los_documentos_digitales.pdf

¹ Electronic Records Archives (ERA): <http://www.archives.gov/era/>

² Strategies to ensure records remain accessible in the long term:

<http://www.naa.gov.au/records-management/secure-and-store/e-preservation/index.aspx>

³ Digital Archive Project: <http://www.prov.vic.gov.au/vers/digitalarchive/development.htm>

⁴ CEDARS: <http://www.leeds.ac.uk/cedars/index.html>

⁵ InterPARES: <http://www.interpares.org/>

⁶ iArxiu: http://www.catcert.net/web/cas/1_4_9_iArxiu.jsp

⁷ El documento completo está accesible en <http://www.csi.map.es/csi/criterios/pdf/conservacion.pdf>

⁸ WORM: Son las siglas, en inglés correspondientes a Write Once Read Many, es decir, escribe una vez y lee cuanto quieras. Esta denominación se concede a medios de almacenamiento (generalmente extraíbles) que tienen esta propiedad: los datos escritos ya no pueden ser borrados o sobre-escritos posteriormente.
<http://es.wikipedia.org/wiki/WORM>

⁹ CRC: La comprobación de redundancia cíclica (CRC) es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento.
http://es.wikipedia.org/wiki/Control_de_redundancia_c%C3%ADclica

¹⁰ Hash: En informática, Hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. <http://es.wikipedia.org/wiki/Hash>

¹¹ Migration: process of transferring electronic document-based information from one software/hardware environment or storage medium to another environment or storage medium with little or no alteration of structure and no alteration in content and context (ISO/TR 18942 – 3 Terms and definitions)

¹² PDF/A: <http://www.pdfa.org/>

¹³ METS: <http://www.loc.gov/standards/mets/>

¹⁴ PREMIS: <http://www.loc.gov/standards/premis/>

¹⁵ The MoReq2 Specification: <http://www.moreq2.eu/downloads.htm>

¹⁶ DoD 5015.02-STD: ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS DESIGN CRITERIA STANDARD: <http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf>

¹⁷ RFC 3126 - Electronic Signature Formats for long term electronic signatures” de IETF (Internet Engineering Task Force) del 2001: <http://www.ietf.org/rfc/rfc3126.txt>

¹⁸ IETF (The Internet Engineering Task Force): <http://www.ietf.org/>

¹⁹ ETSI (European Telecommunications Standards Institute): <http://www.etsi.org/>

²⁰ Documento de apoyo informativo: En contraposición a la documentación de archivo, se considera Documentación de apoyo informativo a aquellos documentos (impresos, fotocopias de disposiciones normativas, folletos, etc.) cuya utilidad para la Administración radica exclusivamente en su contenido informativo para apoyo de la gestión administrativa, por tanto no es documentación susceptible de integración en los expedientes ni de conservación en los archivos. (según la ORDEN de 19 de diciembre de 2005, de la Consejera de Hacienda y Administración Pública, del reglamento del sistema de archivo de la Administración General e Institucional de la Comunidad Autónoma de Euskadi - Artículo 3.– Definiciones y conceptos básicos. http://www.euskadi.net/cgi-bin_k54/bopv_20?c&f=20060217&a=200600843)

²¹ Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común

“Artículo 137. Presunción de inocencia.

3. Los hechos constatados por funcionarios a los que se reconoce la condición de autoridad, y que se formalicen en documento público observando los requisitos legales pertinentes, tendrán valor probatorio sin perjuicio de las pruebas que en defensa de los respectivos derechos o intereses puedan señalar o aportar los propios administrados”

²² Ver el artículo 103 del 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.

²³ Texto extraído del web del Sistema Nacional de Archivos de Euskadi (SNAE): <http://www.snae.org/default.es.php>

²⁴ Para ver el texto completo: http://www.snae.org/pdf/nota_prensa_es.pdf

²⁵ Para ver el texto completo: <http://www.hiru.com/es/artea/erreportaiak/180640>

²⁶ ETSI TS 101 733 V1.7.3 (2007-01) - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES): <http://www.cryptopro.ru/cryptopro/products/tsp/ts-101733v010703p.pdf>