Archivo Digital de la Administración de la Comunidad Foral de Navarra

Modelo de Gestión Documental

Versión 2

Febrero 2014

Índice de contenidos

0 NOTAS DE ESTA VERSIÓN

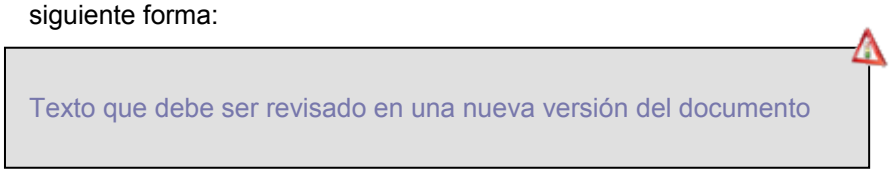
Esta versión del Modelo de Gestión Documental con Archivo Digital supone una revisión del anterior una vez implantada en el Gobierno de Navarra la infraestructura tecnológica que da soporte al archivo digital.

Ello supone:

- Eliminar del Modelo las referencias al plan de implantación del Archivo Digital que ya se ha realizado, dando como resultado ADI (Archivo Digital de la Administración de la Comunidad Foral de Navarra).
- La redefinición de algunas características que se han acordado durante la implantación.

No obstante, a la fecha de cierre de este documento, todavía se encuentra en fase de elaboración y tramitación el *Decreto Foral por el que se regula la digitalización de documentos y el copiado y conversión de documentos electrónicos en el ámbito de la Administración de la Comunidad Foral de Navarra y sus Organismos Autónomos*, lo que exigirá, necesariamente, una revisión de este documento, una vez dicho decreto sea publicado.

Por tanto, todos los textos que tengan relación con este decreto aparecen recuadrados de la siguiente forma:

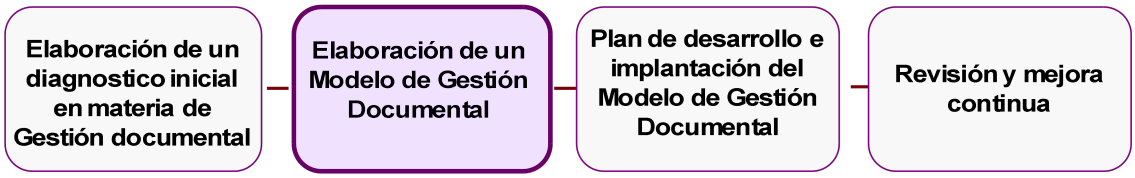


hasta que se redacte la nueva versión de este Modelo.

1 INTRODUCCIÓN

El presente documento describe el Modelo de Gestión Documental del Gobierno de Navarra (en adelante MGD).

Este modelo es uno de los resultados del proyecto de "Sistema de Gestión Documental con Archivo digital" que tenía como objetivo el diseño, la implementación y mejora continua de un sistema para la gestión de los documentos electrónicos.



El MGD constituye el marco de referencia para la gestión de los documentos electrónicos en la Administración de la Comunidad Foral de Navarra. Establece los procesos y las responsabilidades en materia de gestión documental y define las características del Archivo Digital (ADI), que será el instrumento tecnológico que gestionará el conjunto de documentos administrativos electrónicos.

Por tanto el ámbito del MGD es la Administración de la Comunidad con las siguientes puntualizaciones:

- El Modelo se ha elaborado teniendo en cuenta fundamentalmente los requisitos y necesidades de gestión de los documentos electrónicos de la Producción Administrativa, contemplando así mismo un diseño flexible para dar respuesta a otros posibles tipos de documentos electrónicos.
- En materia de Justicia, el Modelo contempla los expedientes de los servicios y funciones traspasados por la Administración del Estado a la Comunidad Foral.
- Los departamentos de Educación y Salud, debido a su singularidad, son objeto de estudio en cuanto a sus unidades de administración general, no contemplándose sus unidades de gestión específicas.

La Metodología seguida para la definición del MGD sigue los principios marcados por las Normas UNE-ISO 15489-1:2006, UNE-ISO/TR 15489-2:2006, UNE-ISO 30300:2011 y UNE-ISO 30301:2011.

2 Conceptos básicos aplicados al Modelo de Gestión Documental

Antes de exponer el modelo de gestión documental del Gobierno de Navarra (MGD), se definen en este apartado los conceptos básicos que se van a manejar, con referencia a algunas de las normas que los definen.

2.1 Documento

El objeto de la gestión que trata este modelo es el documento de archivo, es decir, el creado o recibido por la Administración de la Comunidad Foral en el ejercicio de sus funciones, y específicamente trata del documento electrónico.

DOCUMENTO DE ARCHIVO	
Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos	Toda expresión del lenguaje oral o escrito, natural o codificado, y cualquier expresión gráfica, sonora o en imagen, recogida en cualquier tipo de soporte material, actual o futuro, generada en el ejercicio de la actividad de las personas físicas o jurídicas.
UNE-ISO 15489-1	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.

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

DOCUMENTO ADMINISTRATIVO ELECTRÓNICO	
Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.	Las Administraciones Públicas podrán emitir válidamente por medios electrónicos los documentos administrativos (…), siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Ley 11/2007. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992 (…), así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

2.2 Expediente

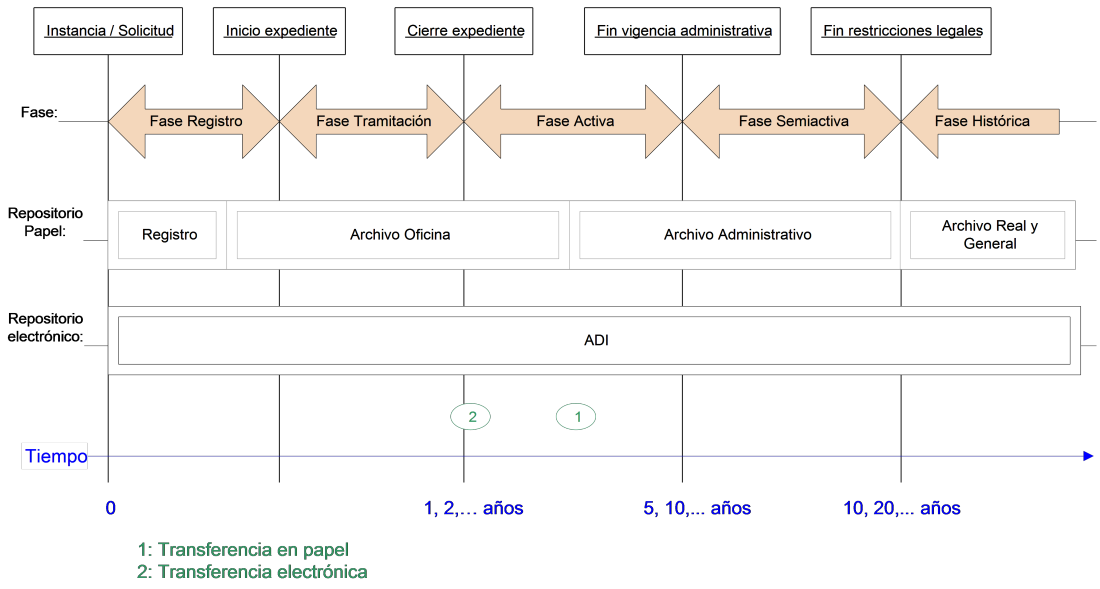
DOCUMENTO ADMINISTRATIVO ELECTRÓNICO	
Ley Foral 11/2007, para la Implantación de la Administración Electrónica.	El expediente administrativo electrónico estará formado por el conjunto de documentos administrativos electrónicos correspondientes a un procedimiento administrativo.

Para garantizar la vinculación de los documentos electrónicos, la legislación define creación de un índice electrónico, que garantiza la integridad del expediente electrónico y permite su recuperación.

2.3 Ciclo de vida de los documentos

CICLO DE VIDA DEL DOCUMENTO ELECTRÓNICO	
Esquema Nacional de Interoperabilidad.	Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Las distintas fases por las que pasa un documento, en la Administración Foral, son:



1: Transferencia en papel
2: Transferencia electrónica

- **Fase de Registro:** es la etapa en la que la documentación ha sido presentada y queda a disposición de las unidades tramitadoras.
- **Fase de Tramitación:** es la etapa en que la documentación está en periodo de tramitación o es de uso habitual por parte de la oficina productora.

En el Sistema Archivístico de la Administración de la Comunidad Foral la gestión de la

documentación activa corresponde a los archivos de gestión o de oficina (los departamentos pueden contar además con archivos centrales)

- **Fase Activa:** en esta etapa la documentación, una vez concluida la tramitación, mantiene valor administrativo y/o legal. No puede modificarse, pero puede ser de uso habitual por la unidad productora, sobre todo a principio de esta fase.

  La gestión de la documentación activa corresponde al Archivo de la Administración de la Comunidad Foral.

- **Fase Semiactiva:** en esta etapa la documentación, una vez concluidos los plazos administrativos y legales que obligaban a su custodia, puede destruirse, excepto aquella que se considere útil para la información o la investigación, que pasará a la fase histórica cuando se libere de restricciones (protección de datos personales, patentes, etc.) que impidan su libre publicación.

  La gestión de la documentación semiactiva corresponde al Archivo de la Administración de la Comunidad Foral.

- **Fase Histórica:** en esta etapa la documentación en fase semiactiva, una vez liberada de sus restricciones legales, se transfiere al archivo histórico, es documentación que se considera útil para la información o la investigación y, por tanto, debe ser conservada con carácter permanente.

  El Archivo Real y General de Navarra es el archivo histórico de la Administración de la Comunidad Foral de Navarra.

3 Gestión documental en la Administración de la Comunidad Foral de Navarra

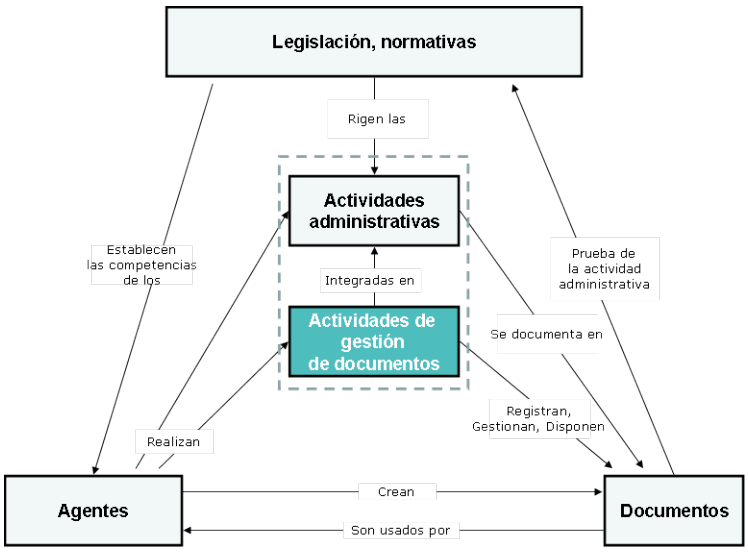
3.1 La gestión documental dentro de la producción administrativa

La Administración de la Comunidad Foral de Navarra se estructura, de acuerdo con el principio de división funcional, en Departamentos que comprenden uno o varios sectores funcionalmente homogéneos de actividad administrativa.

La actividad administrativa se concreta en procedimientos administrativos, regulados por políticas y normativas, en el marco de los cuales las unidades administrativas generan, emiten o reciben documentos.

Por tanto podemos distinguir las siguientes entidades:

- Marco jurídico y normativo: que incluye los procedimientos administrativos establecidos por la Administración de la Comunidad Foral.
- Agentes: principalmente las unidades administrativas que intervienen en la tramitación, pero también sus organismos responsables, los interesados u otras organizaciones.
- Actividades: que incluyen las actividades administrativas, realizadas de acuerdo a los procedimientos administrativos correspondientes, y los procesos necesarios para la correcta gestión documental.
- Documentos



En el caso de los documentos electrónicos, las actividades administrativas y de gestión de documentos se realizan mediante sistemas informáticos, que son analizados a continuación.

3.1.1 Sistemas informáticos

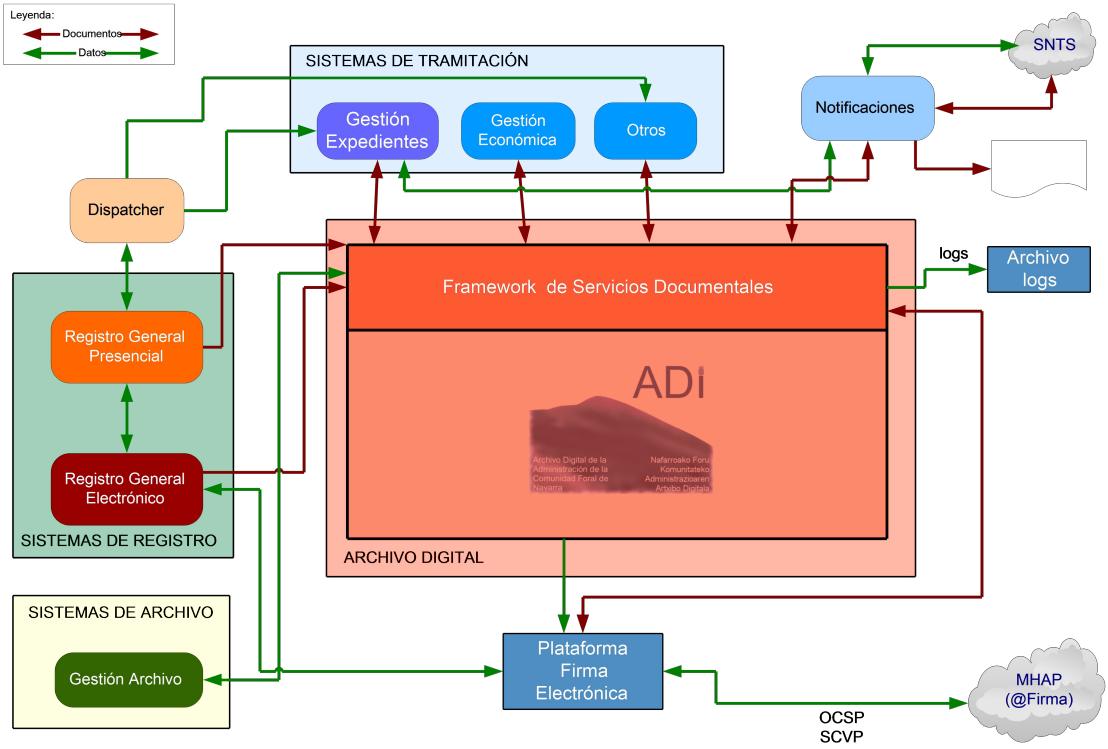
El Gobierno de Navarra cuenta con sistemas, materializados en diversas herramientas informáticas, que dan soporte a las funciones administrativas y que, en relación a su actividad, capturan, generan o emiten documentos electrónicos:

Sistema	Función principal
Registro	Sistema para el registro de entradas y salidas del Gobierno de Navarra
Notificaciones	Sistema de notificaciones del Gobierno de Navarra
Gestión de expedientes	Permite la tramitación y ejecución de los procedimientos administrativos
Gestión de Archivo	Gestiona el archivo de la Administración de la Comunidad Foral de Navarra y su relación con los archivos de oficina
Servicio Centralizado de Firma Electrónica	Plataforma que proporciona servicios de firma electrónica y custodia

Además de estos sistemas, existen otros complementarios como los siguientes:

Sistema	Función principal
Carpeta Ciudadana	La ciudadanía puede consultar datos e información relativa a sus trámites con el Gobierno de Navarra.
Gestión del Conocimiento	Herramienta para el trabajo colaborativo del GN, donde compartir información, documentación, agendas,...
Sistema Integral de Contratación Electrónica	Tramitación electrónica de expedientes de contratación contemplados en la Ley Foral 6/2006 de Contratos Públicos
RRHH	Gestiona la estructura orgánica / RRHH del GN. Nóminas, expedientes personales, gestión de tiempos, turnos, o cualquier tramite sobre el ámbito de los RRHH
Módulo de Compras y Almacenes	Gestión de Compras, y gestión de stocks.

A continuación se presenta gráficamente la comunicación entre los principales sistemas:



3.2 Requisitos de gestión documental

Según determina la Ley Foral 11/2007, la Administración archivará los documentos electrónicos de manera que se pueda verificar más adelante su seguridad, autenticidad e integridad. ADI responde a estos requerimientos:

Integridad

Los documentos que se guarden en ADI estarán protegidos contra modificaciones no autorizadas. Los documentos y expedientes archivados deberán ser completos y no haber sido alterados.

Autenticidad

Para garantizar la autenticidad de los documentos, se controlará la creación, recepción, transmisión y mantenimiento de los documentos.

Se establecerá la relación entre el documento, su productor y el contexto en que se originó.

Los expedientes quedarán clasificados según un sistema de clasificación basado en los procedimientos administrativos que se llevan a cabo en la Administración de la Comunidad Foral.

Los documentos quedarán archivados junto a los metadatos asociados y sus firmas electrónicas. En este sentido, los metadatos contribuyen al valor probatorio y testimonio del documento en la medida en que explican sus circunstancias de creación, gestión y uso.

Seguridad

Los usuarios estarán identificados y autorizados. Los documentos quedarán protegidos de utilización no autorizada y de cualquier adición y/o modificación.

La información no estará disponible o no será revelada a individuos o procesos no autorizados.

El sistema permitirá la configuración de los accesos durante todo el ciclo de vida del documento: usuarios, perfiles y grupos de usuarios, así como permisos diferenciados para la creación, consulta, eliminación, etc.

El sistema controlará y registrará qué acciones se realizan y quién las lleva a cabo.

Fiabilidad y Usabilidad

Los documentos electrónicos estarán disponibles, es decir, podrán ser localizados y recuperados en el curso de posteriores operaciones o actividades. Estarán bien identificados, serán legibles y podrán ser interpretados correctamente.

Conservación

ADI permitirá realizar los procesos y operaciones necesarias para garantizar el mantenimiento de los documentos a lo largo del tiempo

3.3 Contexto normativo

ADI responde a las exigencias legales y normativas que afectan a los documentos electrónicos y su gestión.

3.3.1 Directivas Europeas

Principales Directivas tomadas en consideración:

- **DIRECTIVA 1999/93/CE** DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica
- **DIRECTIVA 2000/31/CE** DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior
- **DIRECTIVA 2010/45/UE** DEL CONSEJO de 13 de julio de 2010 por la que se modifica la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido, en lo que respecta a las normas de facturación

3.3.2 Legislación Foral

Se incluyen en este apartado las normas de la Comunidad Foral de Navarra relativas a la Administración Electrónica, así como la Orden Foral relativa a la Digitalización Certificada de facturas, esta última se relaciona por su importancia al definir los parámetros tecnológicos de un sistema de digitalización considerado seguro y como referencia de los modelos de digitalización.

Especial relevancia tienen la Ley Foral 11/2007, de 4 de abril, para la implantación de la Administración Electrónica en la Administración de la Comunidad Foral de Navarra, y la Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos. La primera de estas normas regula el uso de las Tecnologías de la Información en el ámbito de la Administración Foral y fija las garantías jurídicas derivadas de ese uso para los ciudadanos. Debe señalarse que la propia Ley hace una excepción a su ámbito de aplicación y se atribuye un carácter supletorio en los procedimientos tributarios y en la contratación administrativa, áreas en las que son de aplicación normas especiales. La Ley contiene una habilitación reglamentaria que faculta al Gobierno de Navarra para dictar disposiciones para su desarrollo y ejecución.

La Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos –segunda de las destacadas-, abarca la actuación archivística de la Comunidad Foral de manera global y tiene entre sus objetivos la definición normativa y metodológica de esta actividad.

- **Ley Foral 11/2007**, de 4 de abril, para la implantación de la Administración Electrónica en la Administración de la Comunidad Foral de Navarra.
- **Ley Foral 12/2007**, de 4 de abril, de Archivos y Documentos.
- **Decreto Foral 75/2006**, de 30 de octubre, por el que se aprueba el Reglamento que regula la composición, organización y funcionamiento de la Comisión de Evaluación Documental.
- **Decreto Foral 50/2006**, de 17 de julio por el que se regula el uso de medios electrónicos, informáticos y telemáticos (EIT) en el ámbito de la Hacienda Tributaria de Navarra.
- **Orden Foral 228/2007**, de 12 de junio del Consejero de Economía y Hacienda, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas.
- **Decreto Foral 70/2008**, de 23 de junio, por el que se crea el Registro General Electrónico de la Administración de la Comunidad Foral de Navarra.
- **Ley Foral 15/2009**, de 9 de diciembre, de medidas de simplificación administrativa para la puesta en marcha de actividades empresariales o profesionales.

- **Orden Foral 423/2010**, de 15 de junio del Consejero de Presidencia, Justicia e Interior, por la que se crea la Sede Electrónica de la Administración de la Comunidad Foral de Navarra y sus organismos públicos.
- **Ley Foral 11/2012**, de 21 de junio, de la Transparencia y del Gobierno Abierto.
- **Decreto Foral xx/201x**, de xx de xxx, por el que se regula la digitalización de documentos y el copiado y conversión de documentos electrónicos en el ámbito de la Administración de la Comunidad Foral de Navarra y sus Organismos Autónomos.

3.3.3 Legislación Estatal

De la relación normativa contenida en este apartado destaca la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos. Esta Ley resulta de aplicación con carácter básico a las Comunidades Autónomas y fija la fecha de 31 de Diciembre de 2009 –ya pasada-, como momento a partir del cual los ciudadanos podrán ejercer en estas Comunidades los derechos que se les reconocen en el propio texto.

Real Decreto 1671/2009, de 6 de noviembre, desarrolla la Ley 11/2007 y es de aplicación en la Administración General del Estado. Sin embargo debe ser tenido en cuenta por la importancia de los conceptos y definiciones que contiene, especialmente en lo referido al documento electrónico y las posibilidades de copia, compulsa y destrucción.

La mayor novedad legislativa la constituyen los Esquemas Nacionales de Seguridad e Interoperabilidad. Sin embargo, siendo importantes los conceptos contenidos en los Reales Decretos que contienen estos Esquemas, el nivel mayor de detalle puede encontrarse en las normas técnicas que los desarrollan.

Debe recordarse la vigencia de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en especial de sus artículos 45 y 46. Esta disposición, aunque lejana en el tiempo, sigue siendo referente necesario para determinar el valor de los documentos electrónicos y punto de partida para los conceptos básicos de autenticidad, integridad y conservación.

La Ley 59/2003, de 19 de diciembre de firma electrónica, es relevante por el carácter instrumental de la firma electrónica como medio de garantizar la autenticidad e integridad del documento, sin perjuicio de la utilización de otros sistemas.

La Ley Orgánica de Protección de Datos de Carácter Personal y su reglamento de desarrollo resultan de aplicación tanto para el planteamiento genérico de la Administración Electrónica y el Archivo Digital, como para el cumplimiento concreto de las normas de seguridad.

Por último se destaca la inclusión en esta lista de unas disposiciones con un objeto y ámbito de aplicación muy específico, pero que resultan de gran utilidad para definir usos metodológicos fácilmente replicables en otros ámbitos.

La primera de estas normas es la Orden ITC/1475/2006, de 11 de mayo, sobre utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio, que describe para el ámbito ministerial en exclusiva un sistema que permite eliminar de entrada el papel aportado por los ciudadanos, reteniendo la Administración su imagen electrónica con valor de original.

Las otras normas son las referidas a la digitalización certificada de facturas (Orden EHA/962/2007, de 10 de abril, y Resolución de 24 de octubre de 2007, de la AEAT). Se contiene en estas disposiciones la definición de un método de digitalización y de conservación de documentos electrónicos altamente garantista de la integridad de las imágenes. Este método resulta en principio trasladable a las Administraciones Públicas. En principio y con las debidas salvedades, entre las que se puede plantear la posibilidad de la digitalización externalizada, posibilidad plenamente admitida en el sector privado pero que debe observarse cuidadosamente en el público.

- **Ley 11/2007**, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- **Real Decreto 1671/2009**, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- **Real Decreto 3/2010** de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- **Real Decreto 4/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- **Resolución de 19 de julio de 2011** por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
- **Resolución de 19 de julio de 2011**, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
- **Resolución de 19 de julio de 2011**, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- **Resolución de 19 de julio de 2011**, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración
- **Resolución de 19 de julio de 2011**, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
- **Resolución de 19 de julio de 2011**, por la que se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las entidades registrales.
- **Resolución de 19 de julio de 2011**, por la que se aprueba la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.
- **Resolución de 28 de junio de 2012**, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.
- **Resolución de 28 de junio de 2012**, por la que se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos.
- **Resolución de 28 de junio de 2012**, por la que se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos.
- **Resolución de 3 de octubre de 2012**, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares.
- **Resolución de 19 de febrero de 2013**, por la que se aprueba la Norma Técnica de Interoperabilidad de Reutilización de recursos de información.
- **Ley 59/2003**, de 19 de diciembre, de firma electrónica
- **Ley 7/1985**, de 2 de abril, Reguladora de las Bases del Régimen Local.
- **Ley 30/1992**, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- **Ley 4/1999**, de 13 enero, de modificación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal
- **Real Decreto 1720/2007**, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.
- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **Ley 56/2007**, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
- **Real Decreto 772/1999**, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.
- **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.

- **Ley 30/2007**, de 30 de octubre, de Contratos del Sector Público.
- **Orden EHA/1307/2005**, de 29 de abril, por la que se regula el empleo de medios electrónicos en los procedimientos de contratación.
- **Orden ITC/1475/2006**, de 11 de mayo, sobre utilización del procedimiento electrónico para la compulsa de documentos en el ámbito del Ministerio de Industria, Turismo y Comercio.
- **Orden EHA/962/2007**, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas.
- **Resolución de 24 de octubre de 2007**, de la Agencia Estatal de Administración Tributaria, sobre procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril de 2007.
- **Orden EHA/2784/2009**, de 8 de octubre, por la que se regula la interposición telemática de las reclamaciones económico-administrativas.
- **Ley 37/2007**, de 16 de noviembre, sobre reutilización de la información del sector público.

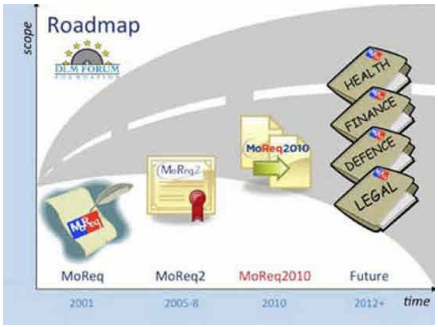
3.3.4 Estándares y normas internacionales sobre gestión documental

Las normas impulsan los procesos de modernización y regulan los aspectos más críticos y fundamentales, como la autenticidad, la preservación, o la eficacia jurídica de los documentos.

Las normativas europeas e internacionales, en especial las normas ISO -International Organization for Standardization-, permiten homologar y consolidar las buenas prácticas, internacionalizar las soluciones y dar cobertura legal a las administraciones más innovadoras.

Entre las más importantes pueden citarse las siguientes:

- **MoReq2010** (Modular Requirements for Records Systems): Sustituye a la versión anterior aprobada en 2008 (Moreq2), y trata de proporcionar una serie de requisitos para un sistema adaptable y aplicable a diferentes sectores.



- **ISO 15489-1 y 145489-2**: Regula la implementación de sistemas de gestión de documentos. La primera parte presenta los principios generales y las políticas que inspiran su aplicación y la segunda ofrece los instrumentos metodológicos y las herramientas que hacen posible su implantación.
- **ISO 30300 y 30301**: Como normas de sistemas de gestión (MSS), proporcionan a la alta dirección de las organizaciones las herramientas necesarias para adoptar un enfoque sistemático y verificable en todo lo relacionado con la creación y el control de los documentos e información procedentes de sus actividades.
- **ISO 14721** (OAIS Open Archival Information System): Define el funcionamiento y las características de un archivo digital. Aborda una amplia gama de funciones incluyendo la ingesta, almacenamiento de archivos, gestión de datos, acceso y difusión.
- **ISO/TR 13028**: Directrices para la implementación de la digitalización de documentos.
- **ISO 23081-1, ISO 23081-2 y ISO/TR 23081-3**: Conjunto de normas pensadas para comprender, implementar y usar metadatos en un contexto de gestión de documentos electrónicos.

- **ISO 16175-1, ISO 16175-2 y ISO 16175-3**: Principios y requisitos funcionales para documentos en entornos electrónicos de oficina.
- **ISO/TR 26122**: Proporciona orientación sobre el análisis de los procesos de trabajo desde la perspectiva de la creación, captura y control de los documentos.
- **ISO 13008**: Guía para la conversión de formatos de documentos electrónicos y para la migración.
- **ISO/TR 15801**: Básicamente este informe técnico se aplica a la documentación electrónica que puede ser requerida como evidencia legal en algún momento.
- **ISO/TR 18492**: Estrategias y buenas prácticas para la conservación a largo plazo de información electrónica basada en documentos del sector público y privado.
- **ISO 14641**: Trasposición de la norma francesa NF Z 42-013 para el archivo electrónico con valor probatorio.
- **PREMIS** Preservation Metadata Implementation Strategies: estándar de metadatos de preservación.
- **ISAD(G)**: General International Standard Archival Description, Norma Internacional General de Descripción Archivística.
- **ISAAR (CPF)**: International Standard Archival Authority Record for Corporate Bodies, Persons, and Families. Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias.
- **ICA-ISDF**: Norma Internacional para la Descripción de Funciones.
- **EAD**: Descripción Archivística Codificada.
- **NEDA**: Norma Española de Descripción Archivística
- **AGRKMS** Australian Government Recordkeeping Metadata Standard (Publicado en 2008). Directrices de aplicación del AGRKMS (Publicado en 2010)
- **UN/CEFACT** United Nations Centre for Trade Facilitation and Electronic Business - Business Requirements Specification.

3.3.5 Normas sobre Protección de Datos y Políticas de Seguridad

La normativa vigente en materia de protección de datos es la siguiente:

- **Ley Orgánica 15/1999**, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD).
- **Real Decreto 1720/2007**, de 21 de Diciembre, de Desarrollo de la Ley Orgánica de Protección de Datos.

El Reglamento de Desarrollo de la LOPD entró en vigor el 19 de abril de 2008 y desarrolla los principios de la Ley Orgánica, y las medidas de seguridad a aplicar en los sistemas de información. Se aplica tanto a ficheros en soporte automatizado, como en cualquier otro tipo de soportes.

Este nuevo Reglamento aúna y completa en un solo documento todas las disposiciones vigentes y aplicables de desarrollo de la Ley Orgánica de Protección de Datos y deroga el Real Decreto 994/1999, de 11 de junio, de Medidas de Seguridad de Ficheros Automatizados.

Esta normativa obliga a todas las Administraciones Públicas a implementar una serie de medidas y procedimientos que garanticen la protección de los datos personales. De acuerdo con la Ley, son datos de carácter personal cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, es decir, toda información que aporte datos sobre una persona física concreta o bien que a través de dicha información se pueda llegar a identificar.

La Ley y su Reglamento de desarrollo mencionan también el concepto de fichero, como cualquier conjunto de datos de carácter personal en cualquier formato

Los datos de carácter personal se dividen en grupos, nivel básico, medio y alto, que requieren la aplicación de diferentes medidas de seguridad y protección para cada grupo.

Junto con la normativa de la protección de datos se seguirán las directrices sobre seguridad del

Esquema Nacional de Seguridad:

El Real Decreto 3/2010, de 8 de enero regula el Esquema Nacional de Seguridad, que tiene como objeto el establecer una política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

El ENS establece una serie de medidas de seguridad que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría del sistema de información de que se trate.

También se contemplan las recomendaciones realizadas en diversas normas internacionales sobre seguridad de la información:

- **ISO 27001**: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.
- **ISO 27002**: Establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.
- **ISO 27037**: Se enfoca a la gestión de evidencias digitales desde el punto de vista de la seguridad de la información. Describe el proceso de reconocimiento e identificación, colección y/o adquisición y preservación de los datos digitales que contienen información de valor evidencial potencial.
- **ISO/TS 21548 y 21547**: exigencias de seguridad para el archivado de expedientes electrónicos de salud.

3.4 Organismos responsables

Se especifican en este apartado los organismos que actualmente tienen competencias en el sistema de gestión documental, determinando sus funciones.

3.4.1 Sistema de Archivo

Ley de la Comunidad Autónoma de Navarra 12/2007, de 4 de abril, de Archivos y Documentos, define el Sistema Archivístico de la Administración de la Comunidad Foral y las funciones de sus integrantes.

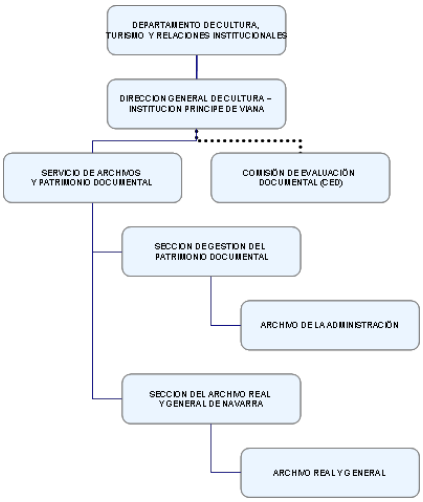
Forman parte del Sistema Archivístico de la Administración de la Comunidad Foral:

Dirección del Sistema:

Desarrolla, entre otras, las siguientes funciones:

- Definir y coordinar la implantación del sistema de gestión documental del Gobierno de Navarra y supervisar su funcionamiento.
- Elaborar la normativa que regule las técnicas de organización, tratamiento, acceso y conservación en cualquier fase del ciclo vital de los documentos

El Servicio de Archivos y Patrimonio Documental (encuadrado dentro de la Dirección General de Cultura del Departamento de Cultura y Turismo) actúa como cabecera del sistema archivístico. (Decreto Foral 126/2007)



Archivo de la Administración

Como archivo intermedio dentro del sistema tiene encomendadas, entre otras, las siguientes funciones:

- Recibe mediante transferencia regular la documentación procedente de los archivos de oficina y de los centrales
- Coordina la aplicación de técnicas archivísticas en los archivos de oficina y en los archivos centrales.
- Elabora los expedientes que se presentan a la Comisión de Evaluación Documental y vela por el correcto cumplimiento de los correspondientes acuerdos y resoluciones.
- Supervisa el correcto cumplimiento de las normas de conservación a lo largo del ciclo vital de los documentos.
- Destruye con anterioridad a su transferencia al Archivo Real y General de Navarra aquellos documentos que se determinen a propuesta de la Comisión de Evaluación Documental.

El Archivo de la Administración se encuadra actualmente en la Sección de Gestión del Patrimonio Documental (Decreto Foral 126/2007)

Archivo real y General

Entre otras funciones, desarrolla las siguientes:

- Recibe mediante transferencia regular la documentación generada o reunida por la Administración de la Comunidad Foral de Navarra en el desempeño de sus funciones que, una vez evaluada y finalizada su vigencia administrativa, se considere que tenga valor cultural y para la investigación.
- Trata técnicamente los fondos documentales bajo su custodia.

Archivos de oficina:

Realizan, entre otras, las siguientes funciones:

- Apoyan las tareas administrativas de la unidad en su ámbito de gestión, en coordinación con el resto de la Administración.
- Clasifican y mantienen debidamente ordenada la documentación, de acuerdo con las normas de la Dirección del Sistema.
- Cumplen los plazos establecidos en el calendario de conservación y transfieren la documentación al archivo central o, en su caso, al Archivo de la Administración.

Las Secretarías Técnicas de los Departamentos tienen entre sus funciones la de establecer los criterios organizativos y coordinar los Registros y Archivos administrativos del Departamento, en colaboración con el resto de las unidades orgánicas competentes en esta materia (Decreto Foral 29/2005).

Archivos centrales:

Tienen asignadas, entre otras, las siguientes funciones:

- Reúnen los documentos procedentes de las distintas unidades administrativas, de acuerdo con los plazos establecidos en las normas de conservación.
- Mantienen organizada la documentación y aplican las técnicas necesarias hasta su transferencia al Archivo de la Administración.
- Destruyen con anterioridad a su transferencia al

Archivo de la Administración aquellos documentos que se determinen a propuesta de la Comisión de Evaluación Documental.

3.4.1.1 Comisión de Evaluación documental

La Ley Foral 14/2005, de 22 de noviembre, de Patrimonio Cultural de Navarra, en su artículo 12, crea la Comisión de Evaluación Documental (CED) como un órgano asesor de la Administración de la Comunidad Foral.

Su funcionamiento y composición están reglamentados por el Decreto Foral 75/2006, de 30 de octubre.

Las funciones de la CED son elevar propuestas, al titular de la Dirección General competente en materia de archivos, relativas a las siguientes materias:

- Determinación de los criterios de evaluación de series documentales para la eliminación o conservación permanente y el acceso a los documentos de archivo.
- Emisión de acuerdos de carácter general relativos a los plazos de conservación o eliminación y acceso para aquellas series comunes a todas las Administraciones Públicas de Navarra.
- Establecimiento, para la Administración de la Comunidad Foral de Navarra, de las etapas de actividad, semiactividad e inactividad de la documentación que produce.
- Fijación para la Administración de la Comunidad Foral de Navarra de los plazos de acceso a los documentos.
- Identificación de los documentos esenciales de la Administración de la Comunidad Foral, que deberán formar parte de un programa de protección, incluido en un plan de prevención de emergencias y desastres.

El Archivo de la Administración tiene encomendada la secretaría de dicha Comisión.

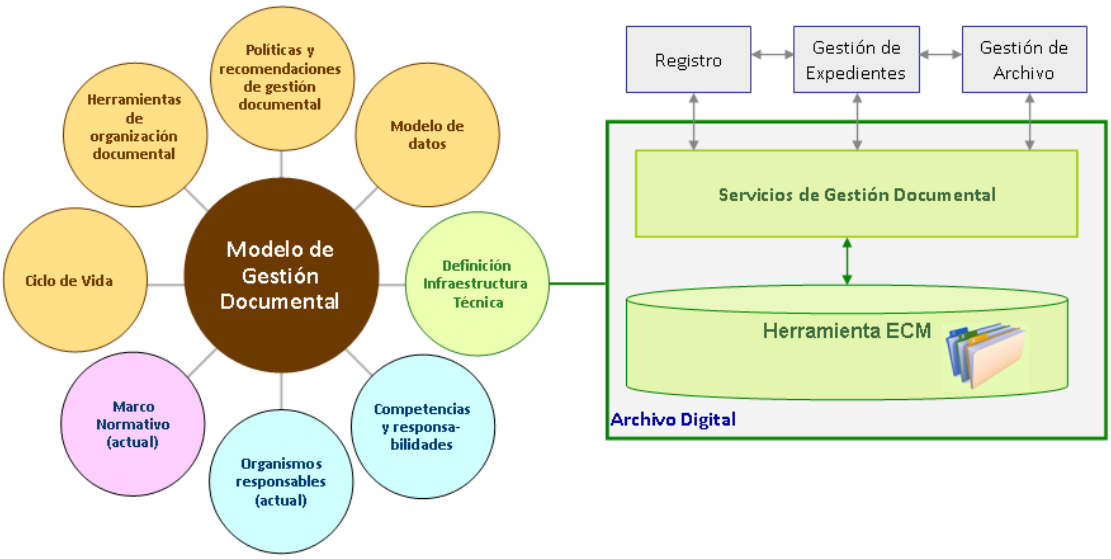
3.4.2 Organización y Tecnología

En el caso de los documentos electrónicos, distintas direcciones generales del Departamento de Presidencia, Justicia e Interior, poseen competencias y responsabilidades:

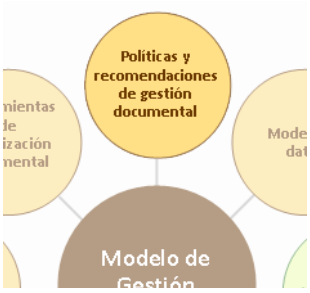
- Organización y modernización.
- Administración y gobierno electrónicos, y en especial, la digitalización de los servicios.
- Sistemas de información. Servicios de informática y de telecomunicación.
- Infraestructuras tecnológicas y soporte a usuarios.
- Seguridad de los Sistemas de Información.

4 Modelo de gestión documental del Gobierno de Navarra

A partir del contexto descrito en los apartados anteriores, en el MGD se desarrollan los aspectos normativos, técnicos y organizativos que deben contemplarse en el sistema de gestión documental de Gobierno de Navarra:



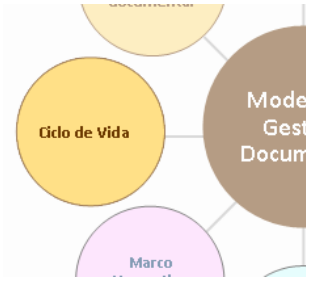
Los elementos del MGD que van a abordarse son los siguientes:



Políticas y recomendaciones en cuanto a la gestión de documentos electrónicos

Estas políticas están encaminadas a optimizar la gestión de los documentos electrónicos con el fin de garantizar su autenticidad, fiabilidad y disponibilidad a lo largo del tiempo.

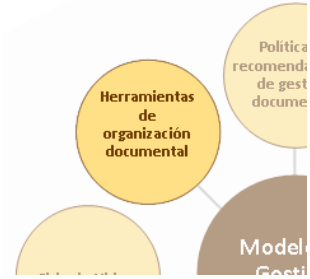
Los documentos electrónicos serán capaces de respaldar, con su valor probatorio, las funciones y actividades del Gobierno de Navarra.



Ciclo de vida

Define el ciclo de vida de los documentos electrónicos del procedimiento administrativo del Gobierno de Navarra.

El ciclo de vida cubre desde el ingreso del documento en el Gobierno de Navarra hasta su eliminación o conservación definitiva, pasando por su tramitación.

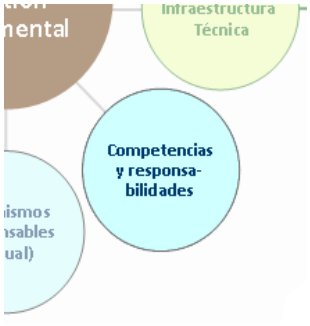


Herramientas de organización documental

Estas herramientas servirán para ayudar a organizar la gestión documental del Gobierno de Navarra.

Entre estas herramientas destacan:

- las tablas de valoración
- el cuadro de clasificación
- las tipologías documentales.



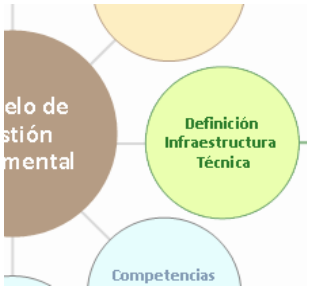
Competencias y responsabilidades

El MGD definirá competencias y responsabilidades para cumplir con las directrices generales del modelo y desarrollar los elementos que todavía no existan.

Modelo de datos

En el modelo de datos, se definirán las distintas categorías y entidades de datos.

Para cada una de estas entidades se definirán los metadatos que permitirán describir el contexto, el contenido y la estructura de los documentos.



Infraestructura técnica

La infraestructura técnica contendrá las herramientas corporativas que soportarán la gestión de los documentos electrónicos del Gobierno de Navarra.

4.1 Ciclo de vida del documento electrónico administrativo

El ciclo de vida del documento electrónico administrativo está formado de las distintas fases por las que atraviesa un documento desde su captura (ingreso en ADI) hasta su disposición final, marcada por la Comisión de Evaluación Documental, y que puede ser la eliminación o la conservación permanente.

En los siguientes apartados se detalla cada una de estas fases en relación con su gestión en ADI.

4.1.1 Registro

La documentación es presentada en el Registro de forma telemática (Registro Electrónico) o bien es aportada por el ciudadano en soporte papel y digitalizada según el procedimiento establecido por Gobierno de Navarra.

Todos los documentos electrónicos (nativos o digitalizados) que entren en el Gobierno de Navarra por medio del Registro se almacenarán en el Archivo Digital. Esto requiere la integración del Sistema de Registro con el Archivo Digital.

En el caso de documentos presentados de forma telemática, los ciudadanos presentan sus solicitudes o comunicaciones por medio del Registro Electrónico, remitiendo una solicitud firmada electrónicamente que contiene referencias (identificadores) a los documentos adjuntos

(anexos), así como los huellas digitales de dichos documentos.

Los documentos electrónicos son incorporados a ADI mediante el proceso de captura.

En el proceso de captura se comprueba que el formato de los documentos es uno de los admitidos y que se han completado los metadatos obligatorios requeridos en los documentos y sus firmas, que previamente han sido verificadas, si así se requiere. La firma de la solicitud siempre se verifica.

Los documentos de esta etapa serán almacenados en ADI señalando que la responsabilidad de la gestión recae en el **Sistema de Registro**

4.1.1.1 Distribución a los sistemas de tramitación

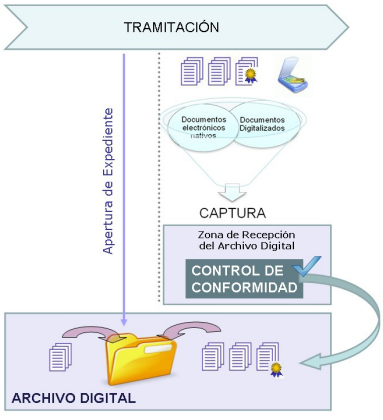
Siguiendo con el ciclo de vida del documento electrónico administrativo, los nuevos asientos registrales, junto con los identificadores únicos de los documentos almacenados en ADI, se distribuyen desde el Sistema de Registro al Sistema de Tramitación. Esto requiere la integración del Sistema de Tramitación con ADI, así como la integración de la herramienta que distribuye los asientos registrales.

- Los documentos provenientes de instancias específicas del Registro Electrónico se distribuyen automáticamente, ya que, desde el momento de su entrada, quedan “clasificados”, es decir, asociados a un procedimiento concreto.
- A los documentos procedentes de otras vías (Instancia general) se les deberá asignar la clasificación en el momento de apertura del expediente.
- Los documentos digitalizados deberán enrutarse al Gestor de Expedientes desde el Sistema de Registro. [Se pueden definir para ello formularios de solicitud con código de barras, códigos QR o similares, para que se automatice su distribución una vez digitalizados]

4.1.2 Tramitación

Siguiendo con el ciclo, el sistema de Registro comunica al Gestor de Expedientes que se ha producido un nuevo asiento registral.

El Sistema de Tramitación de Expedientes abre un nuevo expediente y asigna al mismo los correspondientes documentos. Esto requiere la integración del Gestor de Expedientes Corporativo y otras aplicaciones de tramitación con ADI



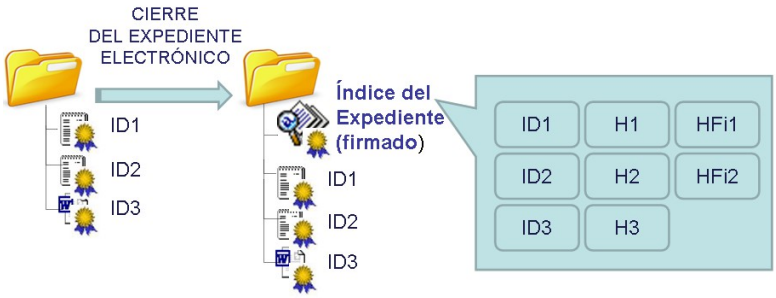
Durante la tramitación del expediente se generan nuevos documentos, que, al igual que los procedentes del Registro, pasan por el proceso de captura e ingresan en ADI.

También se podrá iniciar la tramitación de un expediente directamente desde el Gestor de Expedientes (Inicio de oficio), sin necesidad de incorporar documentos que entren por Registro.

Durante la tramitación se completa la gestión del expediente, llegando a la resolución, y se procede al cierre del expediente.

En este momento se completan los metadatos del expediente, todos los documentos correspondientes quedan correctamente asignados y se genera el índice electrónico. Es en este momento cuando se puede asignar el periodo de conservación (fecha a partir de la cual pueden destruirse los documentos).

El índice, firmado electrónicamente, contiene la identificación de los documentos electrónicos que componen el expediente, a efectos de preservar la integridad del mismo



No podrán incorporarse nuevos documentos a los expedientes cerrados.

No podrán modificarse los documentos de un expediente cerrado

La documentación, una vez concluida la fase de tramitación y cerrado el expediente, mantiene valor administrativo. Su frecuencia de consulta puede ser media/alta por parte de la unidad productora.

Las unidades productoras podrán acceder a los documentos almacenados en ADI a lo largo de todo su ciclo de vida.

Los documentos de esta etapa serán almacenados en ADI señalando que la responsabilidad de la gestión recae en el **Sistema de Tramitación**.

4.1.3 Archivo de la Administración

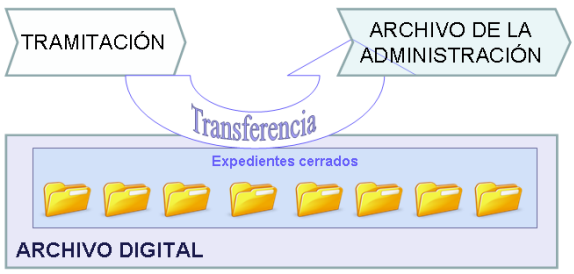
Siguiendo los plazos determinados por el Archivo del Administración, los expedientes le son transferidos desde las unidades productoras.

Los documentos de esta etapa serán almacenados en ADI señalando que la responsabilidad de la gestión recae en el **Sistema de Archivo**. Aunque la unidad productora podrá continuar consultándolos como en la fase anterior

En la gestión documental en papel, son las unidades tramitadoras las que manifiestan la necesidad e interés por transferir documentos al Archivo, liberando así de espacio sus archivos de oficina.

En el mundo electrónico las transferencias son meros cambios de responsabilidad.

La transferencia supone un cambio de responsabilidad sobre el documento transferido, que pasa a ser gestionado por un nuevo organismo responsable.



Respecto a la ubicación de los documentos transferidos, puede seguir siendo la misma desde la captura (un único Archivo Digital, que puede tener diferentes sistemas de almacenamiento) o bien implicar un cambio de ubicación (Archivo Digital distribuido en sistemas que se comunican para la transmisión de documentos). Estos dos modelos de transferencia conviven actualmente en las

Administraciones.

Una vez transferidos los documentos electrónicos al Archivo de la Administración, y según el dictamen de la Comisión de Evaluación Documental, se puede proceder, si así se determina, a la eliminación de los documentos.

El Archivo de la Administración supervisará la destrucción y elaborará las actas de eliminación

4.1.4 Archivo General

El Archivo General recibirá y custodiará los documentos electrónicos para su preservación futura.

Los documentos de esta etapa serán almacenados en ADI señalando que la responsabilidad de la gestión recae en el **Sistema de Archivo General**.

4.1.5 Grado de los documentos: "Preliminar" y "Final"

ADI da soporte a:

- Documentos "preliminales" de trabajo: versiones previas de un documento que se generan durante la tramitación. Son documentos que pueden tener correcciones, ampliaciones y modificaciones, hasta que su contenido queda expresado de forma definitiva.
- Documentos "finales": son expresiones definitivas e inalterables de un documento administrativo electrónico.

El tratamiento de los documentos en ADI es diferente según el grado de los documentos. Son las aplicaciones de gestión y tramitación que incorporan documentos al Archivo las que deben declarar si el documento es "preliminar" o "final".

- Si el documento incorporado ha sido declarado como "Final" y por tanto es un documento definitivo, ADI no dará la posibilidad de versionarlo, ni eliminarlo.
  - Si será posible modificar los metadatos descriptivos del documento, para actualizarlos o corregirlos, sin alterar el contenido del documento.
  - Únicamente se podrá eliminar un documento final cuando así lo indique el Archivo de la Administración, según determine la Comisión de Evaluación Documental.
- Si se trata de un documento "Preliminar" será posible el versionado y borrado del documento, así como la modificación de metadatos.
- Si se trata de un documento firmado también es necesario que se indique desde las aplicaciones de tramitación si se trata de un documento "preliminar" o "final", ya que un documento puede ser firmado en cadena por varias personas y no será considerado "Final" hasta la última firma realizada.

Grado del documento	Versionado	Borrado	Modificación de metadatos descriptivos
Final	NO	NO	SI
Final firmado	NO	NO	SI
Preliminar	SI	SI	SI
Preliminar firmado	SI	SI	SI

Los documentos de Registro son en cualquier caso “documentos finales”
Desde el Gestor de Expedientes se señalará si un documento que vaya a ser guardado en ADI es “Final” o “preliminar”
ADI permitirá señalar un documento “preliminar” como “final” cuando así se indique desde el Gestor de Expedientes

Como paso previo a la firma electrónica de documentos, se realizará, si se solicita la conversión, la transformación de un documento preliminar al formato PDF/A.

En el momento del cierre del expediente, se procederá a la eliminación de los documentos en estado “Preliminar”.

4.1.6 Responsabilidad sobre los documentos

En consonancia con el ciclo de vida del documento, los sistemas de Registro, Tramitación, el Archivo de la Administración o el Archivo General son quienes ostentan la responsabilidad sobre el documento en sus diferentes fases.

La responsabilidad sobre el documento implica:

- asignación de los permisos de consulta, realizada a través de las aplicaciones integradas con ADI.

En la documentación de las fases de Registro y Tramitación son los sistemas de Registro y Tramitación, por medio de las aplicaciones que se integran con ADI quienes facilitan el acceso al documento
En la documentación activa y semiactiva es el Archivo Administrativo, una vez transferidos los documentos, por medio de su aplicación de gestión, quien gestiona las consultas a los documentos, pero se mantiene habilitado el acceso para las unidades tramitadoras
En la documentación histórica es el Archivo General de Navarra quién gestiona las consultas

- Operaciones que afectan al ciclo del documento.

Las Unidades tramitadoras son responsables de declarar qué documentos son “finales” y cuáles son “preliminares”
La responsabilidad del cierre del expediente es de las Unidades tramitadoras o gestoras
El Archivo Administrativo es responsable de destruir aquellos documentos que se determinen a propuesta de la Comisión de Evaluación Documental

5 HERRAMIENTAS DE ORGANIZACIÓN DOCUMENTAL

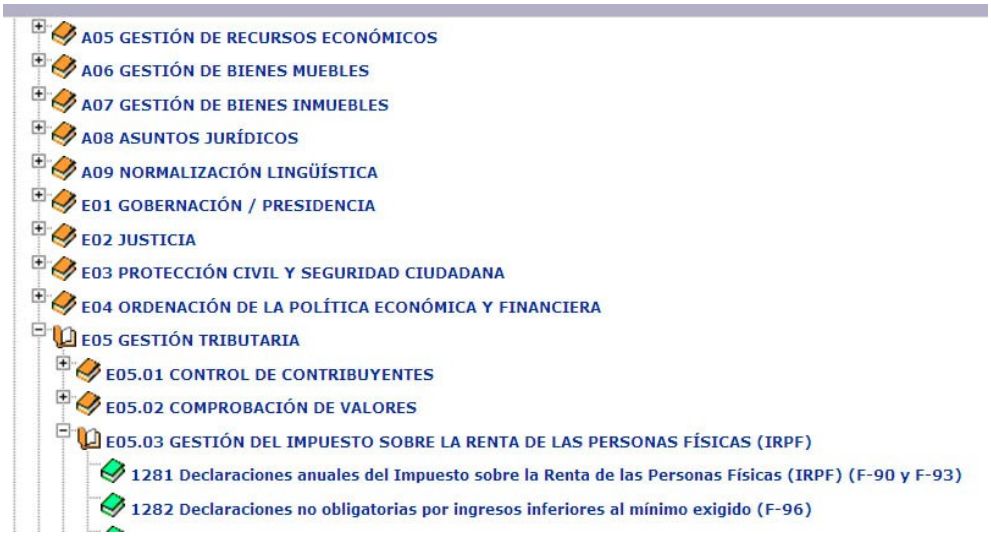
Para gestionar de forma eficiente y unificada todos los documentos administrativos, es necesario contar con herramientas que permitan organizarlos, como el Cuadro de Clasificación, la Valoración Documental y las Tipologías Documentales.

En los siguientes sub-apartados se explica en qué consisten.

5.1 Cuadro de clasificación / Catálogo de Procedimientos

Para organizar y tratar los documentos administrativos de todas las unidades con los mismos criterios y métodos, es importante clasificarlos desde el primer momento del ciclo de vida, a través de un esquema corporativo.

El Archivo de la Administración está desarrollando un sistema de clasificación funcional, donde quedan reflejadas dos categorías de documentos: los documentos de gestión de actividades administrativas, comunes a cualquier organismo, y los documentos de explotación o de gestión de actividades específicas, que corresponden a las funciones precisas que tienen encomendadas las unidades administrativas



El Cuadro de Clasificación plasma las series documentales, es decir, el conjunto de documentos producidos en el desarrollo de una misma actividad administrativa y regulado por la misma norma jurídica y de procedimiento.

Paralelamente existe una clasificación atendiendo a los distintos tipos o familias de procesos que se está plasmando en un Mapa de Procesos.

En ambos casos -Cuadro de Clasificación y Mapa de Procesos-, el último estadio jerárquico es el procedimiento administrativo o serie documental. Por tanto, es esencial recoger e identificar, de forma inequívoca, cada uno de ellos.

Por tanto hay una relación evidente entre estos instrumentos y deben coordinarse en su elaboración y, si en algunos casos no fuera posible una unificación, al menos debe establecerse una relación de equivalencias entre los procedimientos del Mapa y las series del Cuadro de Clasificación.

Todos los expedientes archivados en ADI llevarán indicación del procedimiento administrativo que los ha producido

5.2 Valoración documental

La Valoración documental es el proceso de análisis y determinación de los valores de los documentos en función de los efectos que causan y de la información que contienen. Estos valores (administrativo, legal e histórico) condicionan el destino de los documentos, el establecimiento de plazos para la realización de las transferencias, la decisión sobre su conservación temporal o permanente y los permisos de acceso.

La valoración permite alcanzar los siguientes beneficios:

- Disminución de la masa documental a través de eliminación de documentos, con la consiguiente reducción de los costes de conservación.
- La identificación y protección de los documentos que tienen un valor para el futuro y forman parte del Patrimonio Documental de Navarra
- Los documentos esenciales que son indispensables para la continuidad de la organización en caso de siniestro.
- La garantía de cumplir con el derecho de acceso y el de privacidad de los ciudadanos a los documentos.

La propuesta de evaluación es realizada por los técnicos del Archivo de la Administración de la Comunidad Foral, por iniciativa de la unidad de Archivo o como resultado de la solicitud de la unidad gestora.

Para cada serie documental se elabora una Ficha, según un modelo aprobado por la Orden Foral 252/2007. En la “Ficha de Identificación de Series Documentales” se plasman todos los elementos de juicio (Área de Identificación) y la decisión propuesta (Área de Valoración), que determina los siguientes aspectos:

- Valores Primario (valor administrativo o judicial de la serie) y Secundario (valor para la investigación).
- Transferencia: Establece el plazo (años) en que la documentación papel pasará de una a otra fase de archivo.
- Conservación/Eliminación: Indica la opción de conservación o eliminación y los plazos:
  - Conservación permanente.
  - Eliminación total a los años.
  - Eliminación parcial a los años.
- Acceso: Indica las condiciones de acceso a los documentos:
  - Libre.
  - Restringido.

El resultado del proceso de valoración es una propuesta que debe validar la Comisión de Evaluación Documental mediante un acuerdo que se eleva a la Dirección General de Cultura para su aprobación y posterior publicación en el Boletín Oficial de Navarra.

Los datos sobre la Valoración son plasmados en la aplicación de archivo para la ejecución de las decisiones tomadas:

Ejemplo de datos de una valoración (ArchidocWeb):

Código Valoración:	1124v1
Ordenación Serie Primer Nivel:	Cronológica
Ordenación Serie Segundo Nivel:	Sin orden
Documentos Recapitulativos:	Sistema de Gestión Económica y Financiera (SGEF) (1986-2000) Sistema de Gestión Económica y Financiera (GE-21(SAP) (desde 2001)
Valor Administrativo:	Temporal
Período Vigencia	8 años

Administrativa:	
Justificación:	Orden HAC/1300/2002, de 23 de mayo, por la que se aprueba la Instrucción de Contabilidad para la Administración General del Estado (Título III, Cap. III, regla 24) Regla 24 Conservación de los registros contables. Los registros de las operaciones anotadas en el SIC se conservarán durante un período de seis años, contados desde la fecha de remisión al Tribunal de Cuentas de las cuentas donde se hubiese plasmado la información relativa a dichas operaciones, salvo que por norma de rango suficiente se establezcan otros plazos o se hubiera comunicado la interrupción del plazo de prescripción de la posible responsabilidad contable de acuerdo con lo que se establece en la disposición adicional tercera de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
Valor Legal:	Temporal
Período Vigencia Legal:	8 años
Justificación:	1. Las responsabilidades contables prescriben por el transcurso de cinco años contados desde la fecha en que se hubieren cometido los hechos que las originen. 2. Esto no obstante, las responsabilidades contables detectadas en el examen y comprobación de cuentas o en cualquier procedimiento fiscalizador y las declaradas por sentencia firme, prescribirán por el transcurso de tres años contados desde la fecha de terminación del examen o procedimiento correspondiente o desde que la sentencia quedó firme. 4. Si los hechos fueren constitutivos de delito, las responsabilidades contables prescribirán de la misma forma y en los mismos plazos que las civiles derivadas de los mismos.
Valor Informativo:	No Existe
Justificación:	
Régimen de Acceso:	Restringido Temporal Total
Período de Restricción:	50 años
Justificación:	Para aquella documentación que va a ser eliminada, la restricción alcanza a todo el periodo de su conservación.
Propuesta de Dictamen:	Eliminación Total
Justificación:	

Plazos de transferencia a niveles de archivo:

Nivel origen	Nivel destino	Años del plazo
Oficina	Administrativo	2

Todos los procedimientos administrativos que archiven documentos en ADI deberán estar previamente valorados

5.3 Tipologías documentales

Podemos definir los tipos documentales como la “unidad documental básica, que presenta unas características estructurales similares, derivada del ejercicio de una misma función y producida por un determinado órgano o unidad en el desarrollo de una competencia concreta que viene regulada por una norma de procedimiento”.

Todos los documentos archivados en ADI tendrán indicación del tipo documental al que corresponden

Cada aplicación puede contar con tipos documentales diferentes a los propuestos, por necesidades más específicas de su gestión. **En este caso, se deberá realizar una equivalencia con los tipos documentales ADI**. De esta forma, al almacenar el documento, la aplicación responsable señalaría el tipo documental de destino, sin tener que modificar su gestión habitual

Para la gestión de tipos documentales en ADI, los tipos documentales propuestos son los siguientes:

FAMILIA	TIPO DOCUMENTO (*)	Código	Subtipo
Decisión			
	Resolución	TD01	
	Acuerdo	TD02	
	Contrato	TD03	
	Convenio	TD04	
	Declaración	TD05	
Transmisión_ Comunicación			
	Comunicación	TD06	
	Notificación	TD07	
	Publicación	TD08	
	Acuse de recibo	TD09	
Constancia			
	Acta	TD10	
	Certificado	TD11	
	Diligencia	TD12	
Juicio			
	Informe	TD13	
De Ciudadano dirigido a Administración			
	Solicitud	TD14	
	Denuncia	TD15	
	Alegación	TD16	
	Recurso	TD17	
	Comunicación ciudadano	TD18	
	Comunicación ciudadano (conservación permanente)	TD18_1	Subtipo de TD18
	Factura	TD19	
	Otros incautados	TD20	
Otros			
	Otros	TD99	

(*) En la tabla aparecen en cursiva los tipos documentales propuestos en el Esquema Nacional de Interoperabilidad

6 POLÍTICAS DE GESTIÓN DOCUMENTAL

6.1 Seguridad, firma electrónica y custodia digital

6.1.1 Custodia

El objetivo fundamental de un archivo electrónico es el mantenimiento del valor probatorio de los documentos que custodia. Para mantener este valor probatorio es necesario asegurar la integridad de los documentos electrónicos y de las firmas electrónicas.

Para los procesos de custodia ADI utilizará, además de procesos internos, las funcionalidades de la plataforma de firma electrónica de Gobierno de Navarra.

La custodia se centrará en los siguientes elementos:

- integridad de los documentos electrónicos
- integridad de sus firmas electrónicas
- integridad de las evidencias de validación de las firmas electrónicas

La custodia de los documentos asegurará que los documentos no han sido alterados o modificados indebidamente.

La custodia de las firmas impedirá la modificación de la firma para la que se ha verificado su validez.

La custodia de los informes de las firmas verificadas garantizará la comprobación de la autenticidad de las mismas a lo largo del tiempo.

¿Qué documentos serán custodiados?

Los documentos custodiados serán los documentos finales que genere o reciba la Administración:

Documento	¿Se custodia?
Documento aportado por el Ciudadano	SI
Documento aportado por otras Administraciones	SI
Documento generado por Gobierno de Navarra	SI, en caso de documento final
Documento generado por Gobierno de Navarra	NO, en caso de documento preliminar

Procesos de Custodia:

Custodia de evidencias: permite salvaguardar la integridad del documento custodiado sin requerir de manera obligatoria del documento original. Este tipo de custodia se basa en el mantenimiento de la integridad de las distintas evidencias generadas a partir del contenido original del documento, y de la inclusión de dichas evidencias en un formato de firma avanzado como puede ser XAdES-A

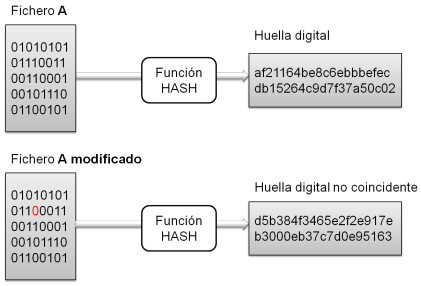
Para llevar a cabo la custodia de evidencias, se calculará el hash del documento con los algoritmos que marque la política de custodia definida en la plataforma de firma y se invocará al servicio de custodia de evidencias de la plataforma de firma, enviándole los hashes calculados y el tamaño de los ficheros a custodiar.

La plataforma de firma generará un XML con esta información, lo firmará en un formato longevo y lo almacenará, devolviendo un identificador a ADI, que lo guardará como un metadato del documento.

Simplificando, un código hash es un conjunto de caracteres que se obtiene a partir del

contenido de un documento electrónico. Un documento electrónico solo puede tener un hash, y un hash solo puede corresponder a un documento.

Estos códigos están generados de tal forma que si se altera en lo más mínimo el documento, el código hash que le corresponde cambia.



6.1.2 Formatos de documentos electrónicos

6.1.2.1 Punto de partida

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, establece los criterios para la selección de los formatos de documentos electrónicos de forma que se garantice la interoperabilidad y la conservación.

Entre otras consideraciones, el ENI establece lo siguiente:

- El documento **se conservará en el formato en que haya sido elaborado, enviado o recibido** y podrá ser convertido en caso de que exista riesgo de obsolescencia.
- Los formatos preferentes corresponderán a un **estándar abierto** y de forma complementaria podrán usarse estándares de uso generalizados por los ciudadanos.
- Los **documentos a disposición de los ciudadanos, se encontrarán, como mínimo, disponibles en estándares abiertos**. Sólo se permitirá el uso en exclusiva de estándares no abiertos en aquellos casos en que no se disponga de un estándar abierto que satisfaga la funcionalidad del formato no abierto.

6.1.2.2 Escenarios de uso y utilización de formatos en la Administración de la Comunidad Foral

Los principales escenarios de uso de los documentos electrónicos en el Gobierno de Navarra son los siguientes:

- Documentos **electrónicos presentados por los ciudadanos** en la Administración (Registro Electrónico).

  Respecto a los formatos admitidos, el Decreto Foral 70/2008 del Registro General Electrónico exige en los documentos anexos a una solicitud, la utilización de formatos que sean compatibles con los utilizados por la Administración de la Comunidad Foral.

  El tipo de formatos compatibles se publican y permanecen actualizados en la dirección http://www.navarra.es (Registro Electrónico)

- Documentos electrónicos **generados por la Administración**.

  No existe normativa en la Administración de la Comunidad Foral sobre la utilización de formatos en la tramitación, pero a través de este Modelo se recomienda la utilización de los formatos explicados más adelante, con el fin de garantizar la conservación futura de los documentos.

- Documentos electrónicos **puestos a disposición o enviados por la administración a los ciudadanos o Administraciones**.

  Habitualmente las notificaciones se realizan mediante documentos en formato pdf y también es el formato preferente para la puesta a disposición de documentos en Sede Electrónica, Carpeta Ciudadana…etc.

Se recomienda utilizar el formato PDF/A.

- Conversión de formatos obsoletos almacenados en el ADI.

  Como formato de conservación a largo plazo se recomienda la utilización del formato PDF/A.

6.1.2.3 Formatos analizados

En este apartado se recogen los formatos propuestos como idóneos, teniendo en cuenta los recomendados en la Norma Técnica de Interoperabilidad del Catálogo de Estándares.

Se admiten algunos formatos de audio y vídeo, aunque la mayor parte de los documentos administrativos son actualmente texto o imagen.

Formatos de texto e imagen	
TXT ANSI, Unicode, UTF-8 Fichero de texto plano	Fichero de texto plano. Especificación abierta. Muy extendido. Es uno de los formatos admitidos en el Registro General Electrónico
RTF Rich Text Format	Formato desarrollado por Microsoft, que mantiene la propiedad intelectual. Es un formato bastante extendido, aunque su uso cada vez es menor. Es uno de los formatos admitidos en el Registro General Electrónico
OD Open Document	ISO/IEC 26300. Especificación abierta de acceso libre. Formato de fichero estándar para el almacenamiento de documentos ofimáticos (documentos de texto, hojas de cálculo, presentaciones,…). En el Registro General Electrónico se admiten los formatos ODS (hoja de cálculo) y ODT (texto). Al implantarse LibreOffice en Gobierno de Navarra, los órganos administrativos pueden generar además presentaciones (ODP) o imágenes (ODG) con esta herramienta.
PDF Portable Document Format	ISO 32000. Formato abierto de documento portátil. Versión mínima aceptada: 1.4 Admitido en el Registro General Electrónico de Navarra.
PDF/A Formato PDF para archivo (conservación a largo plazo)	ISO 19005. Especificación abierta. Formato de archivo de documentos electrónicos para conservación a largo plazo Un archivo PDF/A debe estar 100% auto-contenido, toda la información necesaria para mostrar el documento estará presente en el fichero.
XML eXtensible Markup Language	Estándar W3C. Uso muy generalizado. XML se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo,…
HTML HypertText Markup Language	Estándar W3C. Uso muy generalizado. Es un lenguaje de marcado diseñado para estructurar textos y presentarlos en forma de hipertexto. Versión mínima aceptada 4.01
XHTML eXtensible HyperText Markup Language	Es básicamente HTML expresado como XML válido
CSS	Lenguaje usado para definir la presentación de un documento estructurado escrito en HTML o XML. Versión mínima aceptada 2.1
CSV	Especificación abierta. Los ficheros CSV permiten representar

Formatos de texto e imagen	
Comma-Separated Values	datos en forma de tabla, en las que las columnas se separan por comas (o punto y coma) y las filas por saltos de línea. Formato admitido en el Registro General Electrónico de Navarra.
OOXML Office Open XML	ISO/IEC 29500 Formato creado y desarrollado por Microsoft. Es un formato de archivo abierto para documentos ofimáticos. El formato de texto (DOCX) y el de cálculo (XLSX) están admitidos en el Registro General Electrónico
MS Office (6.0-2003) *Estos formatos no están admitidos en el Catálogo de Estándares	Microsoft Office utiliza formatos nativos propietarios cerrados y muy utilizados. En la Administración de la Comunidad Foral está ampliamente extendido. El formato de texto (DOC) y el de cálculo (XLS) están admitidos en el Registro General Electrónico
JPG/JPEG Joint Photographic Expert Group	ISO/IEC 15444 JPEG 2000 es una norma de compresión de imágenes basada en transformación de ondas. Su objetivo fue el de mejorar el algoritmo JPG. JPG es el formato de imagen más común utilizado por las cámaras fotográficas digitales y otros dispositivos de captura de imagen. Es un formato admitido por el Registro General Electrónico de Navarra
PNG Portable Network Graphics	ISO/IEC 15948. Especificación abierta. Bastante extendido. Formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps.
SVG Scalable Vector Graphics	Especificación para describir gráficos vectoriales. Formato abierto, estándar y basado en XML
TIFF Tagged Image File Format	ISO 12639. Formato abierto. Extendido. Permite documentos multipágina. Admitido en el Registro General Electrónico de Navarra.
XSN	MS InfoPath, utilizado por el Gestor de Expedientes Corporativo.

Formatos de compresión de ficheros	
Zip	Especificación abierta. Admitido en el Registro General Electrónico de Navarra

Formatos de audio	
MP3 MPEG-1 Audio Layer 3	ISO/IEC 11172 Formato muy extendido. Formato de compresión de audio digital que usa un algoritmo con pérdida para conseguir un menor tamaño de archivo. Es un formato de audio común usado para música tanto en ordenadores como en reproductores de audio portátil.
Ogg/Oga	Es un formato abierto y libre de patentes. Los codecs Ogg han sido incluidos en gran cantidad de reproductores

Formatos de vídeo y contenedores multimedia	
H.264/MPEG-4 AVC	Estándar de codificación de vídeo. Es un formato actualmente más empleado para difusión de video online.

Formatos de vídeo y contenedores multimedia	
MPEG-4	MPEG-4 es una técnica de compresión de vídeo desarrollada por MPEG. Es estándar ISO/IEC 14496. Los formatos DivX o Xvid utilizan esta técnica de compresión. Es un formato muy extendido. La versión mínima aceptada corresponde a 2003
AVI Audio Video Interleave	No es un estándar abierto. Muy extendido. Es un formato contenedor de audio y video creado por Microsoft. Existen multitud reproductores que permiten visualizar este contenedor, aunque necesitarán los codecs de los formatos de video y audio.

6.1.2.4 Propuesta de formatos a utilizar

Documentos presentados por los ciudadanos

Los admitidos en el Registro General Electrónico

(http://www.navarra.es/home_es/Servicios/ficha/1718/Registro-General-Electronico)

Tipo	Formatos admitidos	
Texto e imagen	CSV	RTF
	DOC / DOCX	TIFF / TIF
	JPG / JPEG	TXT
	ODS	XLS / XSLX
	ODT	
	PDF	
Compresión de ficheros	ZIP	

Documentos generados por la administración.

Se contemplan diversos formatos de ficheros que pueden ser editados por los técnicos del Gobierno de Navarra con el fin de que puedan ser modificados, y utilizados para la creación de nuevos documentos.

Se recomienda que los documentos finales se conviertan a PDF/A antes de su firma y almacenamiento en ADI.

Tipo	Formatos admitidos	
Texto e imagen	CSV	TIFF / TIF
	DOC / DOCX	TXT
	JPG / JPEG	XLS / XSLX
	ODS	XML
	ODT	HTML, HTM, XHTML
	ODG	HTM
	PDF	CSS
	RTF	PNG
		SVG

Documentos puestos a disposición o enviados por la administración a los ciudadanos o Administraciones

Estos documentos no pueden ser modificados. Como criterio clave es importante que su lectura sea gratuita para el ciudadano, y que pueda utilizar un estándar abierto.

Como formato para los documentos enviados a la ciudadanía por el Gobierno de Navarra se recomienda se recomienda la utilización del formato **PDF/A**.

Tabla resumen de formatos propuestos

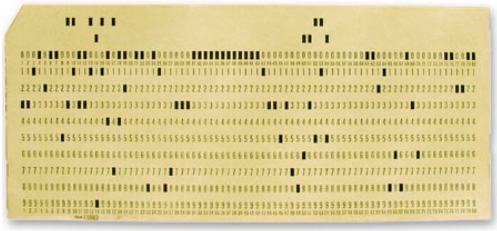
Escenario	Formatos admitidos
Documentos presentados por los ciudadanos	**Texto e imagen** CSV, ODS, RTF, XLS / XSLX DOC / DOCX, ODT, TIFF / TIF, ZIP JPG / JPEG, PDF, TXT
Documentos generados por la Administración	**Texto e imagen** CSV, ODT, TIFF / TIF, HTML, HTM, XHTML DOC / DOCX, ODG, TXT, CSS JPG / JPEG, PDF, XLS / XSLX, PNG ODS, RTF, XML, SVG Se recomienda que: o los documentos finales se conviertan a PDF/A antes de su firma y almacenamiento en ADI o los documentos CAD se conviertan a formatos de lectura (PDF/E) antes de su almacenamiento en ADI. o Las presentaciones, en sus diferentes formatos (PPT, ODP, PPTX…), se conviertan a PDF antes de su almacenamiento en ADI
Documentos puestos a disposición o enviados por la administración a los ciudadanos o Administraciones	PDF/A
Conversión de formatos obsoletos almacenados en ADI	Como formato de conservación a largo plazo: PDF/A

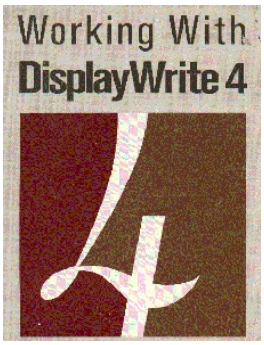
Se recomienda utilizar, siempre que sea posible, el formato PDF/A.

6.1.3 Preservación de documentos electrónicos

La preservación digital presenta una serie de problemáticas, relacionadas con los formatos y la obsolescencia de la tecnología. Los formatos de software, y los soportes donde se almacenan los documentos electrónicos se vuelven ilegibles con el paso del tiempo.

A medida que se suceden nuevas generaciones de hardware y software los documentos dejan de ser accesibles.





Los problemas no son únicamente de carácter técnico, sino que también tienen otras dimensiones, organizativas y económicas, ya que la Administración tiene la responsabilidad de conservar la información durante largos periodos de tiempo.

Un dato importante a tener en cuenta es que no existe hoy en día una solución integral que ofrezca las funcionalidades necesarias para la preservación digital, de manera que se deben de utilizar diversas herramientas, algunas de ellas aún no consolidadas.

6.1.3.1 Programa de preservación digital

El sistema de preservación de documentos electrónicos será proactivo. Es decir, se deberá monitorizar periódicamente el entorno actual de software y hardware para averiguar si alguno de los formatos de software en los que se almacenan los ficheros, o los soportes de almacenamiento, han llegado a ser obsolescentes o problemáticos.

El programa de vigilancia contemplará los siguientes aspectos:

- Mecanismos para la monitorizar la viabilidad de formatos y soportes.
- Criterios de evaluación de formatos: plazo de conservación de los documentos, usuarios y fines de acceso a los documentos, plataformas y tecnologías en que deben estar accesibles…etc.
- Criterios de evaluación de soportes.
- Dictamen sobre intervención.
- Seguimiento del proceso del cambio y validación de la intervención.

El equipo responsable del programa de preservación digital será multidisciplinar, formado por técnicos informáticos y responsables del Archivo de la Administración y del Archivo General de Navarra.

6.1.3.2 Control de formatos: normalización y migración

Para poder realizar las actividades de conservación es necesario seleccionar ciertos tipos de formatos, que por sus características técnicas, sean los más adecuados para almacenar los ficheros y firmas que componen los documentos.

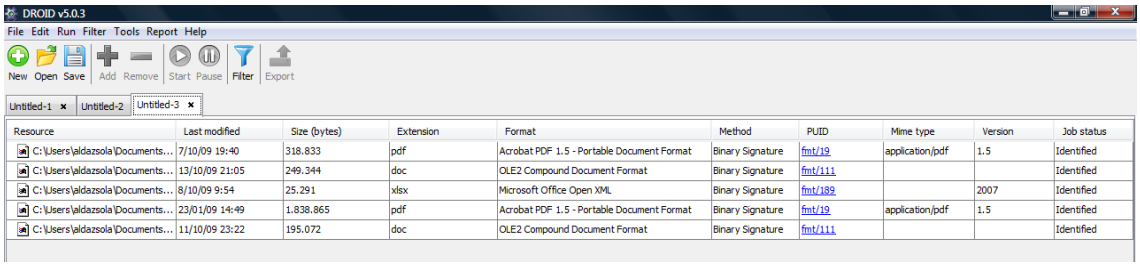
Es decir, ADI no puede asumir todos los tipos de formatos existentes, debe aceptar un número reducido (normalización) y realizar labores de vigilancia, que permitan advertir la necesidad de migrar un determinado formato.

En el esquema de metadatos se propone recoger la información sobre el formato del fichero, como un dato clave para la gestión futura de los documentos. La información sobre el formato se recogerá desde el momento de la captura del documento electrónico:

- A lo largo de los años, los ficheros posiblemente sufrirán migraciones y otras transformaciones técnicas para garantizar su permanencia futura. Para la gestión de estos procesos será imprescindible conocer los formatos y otras características técnicas iniciales de los ficheros.

El problema del control de formatos es universal, de ahí que distintas instituciones hayan reaccionado creando herramientas que permitan disponer de un sistema fiable para la identificación de los formatos.

ADI utilizará inicialmente la herramienta DROID, creada por los Archivos Nacionales del Reino Unido y que permite la identificación de formatos de ficheros.



Resource	Last modified	Size (bytes)	Extension	Format	Method	PUID	Mime type	Version	Job status
C:\Users\aldazsola\Documents...	7/10/09 19:40	318.833	pdf	Acrobat PDF 1.5 - Portable Document Format	Binary Signature	fmt/19	application/pdf	1.5	Identified
C:\Users\aldazsola\Documents...	13/10/09 21:05	249.344	doc	OLE2 Compound Document Format	Binary Signature	fmt/111			Identified
C:\Users\aldazsola\Documents...	8/10/09 9:54	25.291	xlsx	Microsoft Office Open XML	Binary Signature	fmt/189		2007	Identified
C:\Users\aldazsola\Documents...	23/01/09 14:49	1.838.865	pdf	Acrobat PDF 1.5 - Portable Document Format	Binary Signature	fmt/19	application/pdf	1.5	Identified
C:\Users\aldazsola\Documents...	11/10/09 23:22	195.072	doc	OLE2 Compound Document Format	Binary Signature	fmt/111			Identified

6.1.3.3 Selección de formato de conservación

Actualmente el formato más extendido para la preservación digital es el PDF/A

Existen diversas versiones de la especificación:

- PDF/A-1a y PDF/A-1b (más simple de obtener, pero con menos garantías del nivel de conformidad de Archivo).
- PDF/A-2, que moderniza el estándar.

La mayor parte de los formatos de texto e imagen pueden ser convertidos a PDF/A.

En cuanto a los formatos audiovisuales, la selección de un formato de conservación es más compleja, ya que suelen estar constituidos por un “contenedor” que encapsula varios códec (que pueden ser audio y/o vídeo).

Hoy en día el formato más recomendable para el archivado es el siguiente:

- Contenedor MPEG-4 (Ver el apartado de formatos admitidos)

Otro tipo de formatos comunes en la Administración son los diseños técnicos por ordenador (CAD).

ADI no tiene por objetivo guardar información de tipo CAD. Dicha información debe ser guardada y conservada en el ámbito de las herramientas que la generaron puesto que poseen funcionalidades que permiten la gestión de la información contenida en estos formatos.

ADI puede guardar representaciones (documentos finales) de dicha información almacenadas en ficheros de imagen o PDF. Estas representaciones, si bien pierden la capacidad de edición de la información y –a veces- información del contenido, son adecuadas para ser consultadas independientemente de la plataforma que las creó.

Para estos casos el formato recomendado actualmente es PDF/E (ISO 24517).

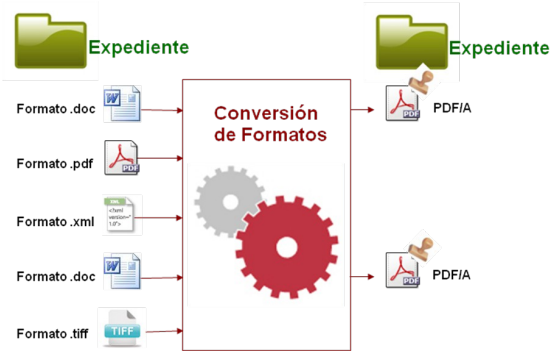
6.1.3.4 Conservación de bases de datos

Cierto tipo de información, como la fiscal o contable o los registros oficiales, suele conservarse en bases de datos. Han sustituido, de hecho, a los libros de registro.

Aunque cabría la posibilidad de archivar en ADI las historificaciones de bases de datos, de momento, no se contempla. Además sería recomendable que se exporte de forma que encaje en los tipos de datos definidos anteriormente y que se pueda recrear posteriormente (datos, modelo de datos, modelo lógico y físico, diagramas entidad-relación…).

6.1.3.5 Conversión de formatos

Para asegurar la accesibilidad de los documentos en el tiempo, se convertirán los formatos si se detecta riesgo de que no sea legible (riesgo de obsolescencia).



Ejemplo de normalización de formatos: ante el riesgo de obsolescencia de un documento electrónico en formato Word 98, se realiza su conversión a formato pdf/a.

6.1.3.6 Proceso de conversión de formatos obsoletos

ADI ofrece un servicio que permite la conversión de formatos obsoletos.

Antes de la llamada a este servicio de conversión, es imprescindible que se planifiquen y realicen de forma adecuada los siguientes pasos:

- Planificación:
  - Determinar qué formato es el que debe convertirse y cuál es el formato destino
  - Identificar qué tipo de enlaces o vínculos del documento pueden quedar comprometidos con la conversión.
  - Identificar si pueden existir componentes en un documento que deben ser convertidos al mismo tiempo (por ejemplo una imagen incrustada en un documento de texto)
  - Determinar qué elementos de la representación del documento (capas, elementos gráficos, etc.) son parte importante de los mismos y deben ser convertidas.
- Pruebas.
  - Antes de realizar el proceso de conversión se deben realizar las pruebas que verifiquen si la conversión no produce pérdida de información o cambios indeseados.
- Conversión. En el proceso de conversión es aconsejable realizar las siguientes actividades:
  - realizar una copia previa de los documentos a migrar, de forma que si algo va mal el proceso no sea irreversible.
  - si en el proceso de conversión se detectan daños o pérdidas, documentar las decisiones tomadas.
- Autenticación de copia
  - Para avalar la autenticidad de la copia resultante del proceso, sobre los documentos convertidos se aplicará una firma electrónica.
- Validación
  - Comprobar que el proceso se ha realizado sin errores.
  - Comprobar que en los metadatos de los ficheros convertidos figura el carácter de copia correspondiente y el vínculo con el documento origen.
  - Comprobar que en la auditoría del sistema quedan reflejadas las operaciones realizadas.

Todas estas fases deben quedar documentadas incluyendo informes de error, comprobaciones, etc.

La información que debe recogerse es la siguiente:

- Documentación realizada sobre las pruebas y sobre los formatos origen y destino.
- la autorización de la persona responsable en conversión de formatos y fecha de autorización.
- la fecha de realización de la conversión.
- los ficheros afectados por la conversión.

6.1.3.7 Prevención de degradación de soportes

Para evitar la pérdida de los registros debido a la degradación del soporte de almacenamiento, es necesario establecer un refresco periódico que asegure la legibilidad continuada.

El refresco debe realizarse a intervalos regulares que no deben nunca superar los periodos recomendados por los fabricantes de los dispositivos.

Si se determina que el soporte de almacenamiento utilizado para la custodia ya no es el apropiado, debe establecerse una migración de soportes. La migración difiere del refresco en que los documentos electrónicos son reescritos en un soporte diferente al inicial.

Tras un proceso de refresco o migración se debe realizar una verificación mediante una comparación de bits entre la versión original y la de destino de cada uno de los ficheros.

6.1.4 Seguridad

La Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece en su artículo 31.3:

> *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****.*

Las medidas de seguridad a implementar que impone la normativa se especifican en:

- Medidas de seguridad LOPD
- Medidas de seguridad ENS.

El Esquema Nacional de Seguridad contempla la categorización de los sistemas de información en 3 escalones, en función del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios en alguna de las dimensiones de seguridad: autenticación, integridad, confidencialidad, disponibilidad y trazabilidad.

El modelo de seguridad de ADI, siguiendo las medidas de la LOPD y del ENS, se soporta en buena medida en la restricción de acceso a la documentación almacenada en el servidor de contenidos, a través de la definición y la relación de usuarios, roles, grupos de seguridad y/o cuentas.

Cada uno de los documentos almacenados en el sistema pertenece a un grupo de seguridad y tiene asignada una cuenta que restringe las operaciones permitidas sobre el mismo.

Existe un grupo de seguridad por cada uno de los estados del ciclo de vida. De este modo cada documento puede evolucionar sus permisos en función del ciclo de vida, y los sistemas no varían su gestión en llamadas a ADI, sino que es el propio sistema de gestión documental quien se encarga de asignar los permisos de la fase correspondiente.

Se han habilitado cuentas para restringir el acceso a la documentación a nivel de aplicación, de tal manera que a través de la asignación de cuentas a los documentos se contemple la existencia de:

- Documentación pública de una aplicación.
- Documentación privada de una aplicación.
- Documentación compartida entre una o varias aplicaciones, pertenezcan a la misma entidad o a diferentes entidades.

- Documentación pública para todas las entidades de la organización.
- Documentación, de cada una de las tipologías anteriores, que tenga que ser accesible por las aplicaciones horizontales registro y notificaciones.

Para cada aplicación susceptible de insertar documentos en ADI se crearán 2 cuentas, una para sus “documentos públicos”, es decir que puede ser compartida con otras aplicaciones y otra para sus “documentos privados”

Por otra parte las aplicaciones que accedan a los documentos de ADI podrán establecer los documentos como de Libre Acceso o Acceso Restringido según corresponda.

En cualquier caso conviene aclarar que el acceso de los usuarios a ADI no se realiza directamente, sino a través de las aplicaciones que le relegarán la gestión de sus documentos. Por tanto, el control de acceso dependerá también en última instancia del sistema de identificación, autenticación y autorización implementado en las aplicaciones.

Todas las comunicaciones entre las distintas aplicaciones y ADI se protegen mediante el protocolo SSL, de forma que la información viaja cifrada.

Los usuarios y contraseñas utilizados por ADI se almacenan debidamente cifrados.

Por otro lado, queda almacenada información de trazabilidad en las interacciones con los documentos, de manera que pueda cumplirse con las medidas de seguridad contempladas en la normativa. Se ha determinado qué datos de trazabilidad se almacenarán, qué operaciones se auditarán y el modelo de datos asociado.

En cuanto a las copias de seguridad, las copias realizadas serán alojadas de manera que permitan recuperar datos perdidos accidental o intencionadamente.

Los datos de respaldo disfrutan de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.

ADI utilizará funciones criptográficas proporcionadas por la Plataforma de Firma de Gobierno de Navarra, para garantizar aspectos como la custodia y retención segura, la comprobación de la firma electrónica de los documentos que hayan sido firmados, el sellado de tiempo,… Por tanto, gozará de integración con la misma.

Todos los elementos de seguridad se describen en detalle en el “Modelo de Seguridad de ADI”.

6.1.5 Firma electrónica

En este apartado se definen las reglas y obligaciones de todos los actores intervinientes en los procesos de generación y verificación de firma, estableciendo la información que debe incluir el firmante y la que debe comprobar el verificador al validar la misma.

Se utiliza como referencia la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, así como la política de firma electrónica de la AGE.

6.1.5.1 Firma electrónica: definiciones

La Ley 59/2003 define firma electrónica, firma electrónica avanzada y firma electrónica reconocida:

*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.

Para que una firma electrónica sea firma electrónica avanzada debe cumplir los requisitos de:

- Autentificación o identificación del firmante. Permite garantizar la identidad del firmante de forma única.
- Integridad de la información firmada. Garantiza que los datos firmados han permanecido completos y no han sufrido alteraciones
- No repudio de lo firmado. Es la garantía de que no puedan ser negados los datos firmados.

Por otra parte, la citada Ley 59/2003, de 19 de diciembre, define el **certificado electrónico** distinguiendo los siguientes conceptos:

*Un **certificado electrónico** 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.*

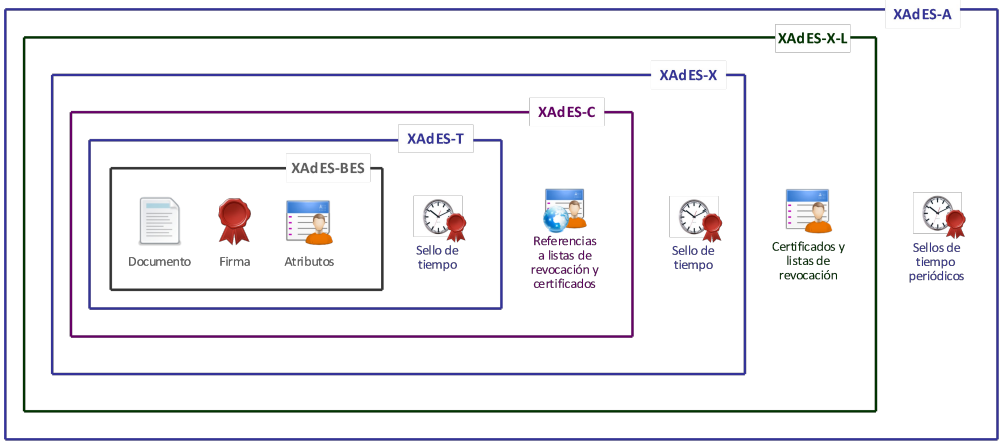
*Son **certificados reconocidos** los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios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

De manera general, el formato de los documentos electrónicos con **firma electrónica reconocida** se deben ajustar a los estándares europeos (ETSI - European Telecommunications Standards Institute) relativos a los formatos de firma electrónica:

XAdES (**X**ML **Ad**vanced **E**lectronic **S**ignatures)	Especificación técnica: ETSI TS 101 903 Versión mínima aceptada 1.2.2 y versión 1.3.2
CAdES (**C**MS **Ad**vanced **E**lectronic **S**ignatures)	Especificación técnica: ETSI TS 101 733 Versión mínima aceptada: 1.6.3
PAdES (**X**ML **Ad**vanced **E**lectronic **S**ignature)	Especificación técnica: ETSI TS 102 778 Versión mínima aceptada: PAdES-1 1.1.1 PAdES-3 1.1.2 PAdES-4 1.1.2.

Para estos formatos se definen clases que incrementan el nivel de protección ofrecido:

- BES: forma básica.
- EPES: añade información sobre la política de firma.
- T (timestamp): añade sellado de tiempo avalado por una TSA.
- C (complete): añade referencias a datos de verificación (certificados y listas de revocación).
- X (extended): añade sellos de tiempo a las referencias, para evitar que pueda verse comprometida en el futuro una cadena de certificados.
- X-L (extended long-term): añade los propios certificados y listas de revocación a los documentos firmados.
- A (archivado), añade la posibilidad de timestamping periódico. Este proceso de resellado deberá repetirse antes de que caduque el sello de tiempo.



6.1.5.2 Firma de los documentos administrativos

En cuanto a la firma de documentos administrativos electrónicos de ADI se contemplan dos escenarios de utilización:

- Documentos aportados por los ciudadanos, a través de los sistemas de Registro. En concreto a través del Registro General Electrónico (RGE).
- Documentos administrativos aportados o generados durante la tramitación, a través las aplicaciones de gestión, por ejemplo el Gestor de Expedientes Corporativo (Extr@).

La Ley Foral 11/2007 para la Implantación de la Administración Electrónica en la Administración de la Comunidad Foral de Navarra establece los requisitos de firma de autoridades, funcionarios e interesados.

6.1.5.3 Plataforma de Firma Electrónica

El Gobierno de Navarra cuenta con una Plataforma de Firma Electrónica que ofrece diversas utilidades: sellado, verificación de certificados, identificación de firmas, cifrado, descrifado...

Dicha plataforma proporcionará estas utilidades a los diferentes sistemas que los invoquen (Sistema de Registro, Sistema de Tramitación…) aunque inicialmente solo serán de aplicación los siguientes:

- Generación de firmas electrónicas hasta el perfil –A, lo que permite soportar firmas longevas.
- Verificación de firmas electrónicas en los formatos recomendados por la NNTT de Interoperabilidad, XAdES, CAdES y PAdES.
- Custodia de evidencias

ADI no firma digitalmente ni verifica la validez de las firmas electrónicas de los documentos que se le proporcionan y se apoyará en los servicios que ofrece la Plataforma de Firma Electrónica para la custodia.

Las aplicaciones que quieran almacenar la validez de una firma deberán validarla contra la Plataforma de Firma y almacenar tanto el documento firmado como la validación obtenida.

6.1.5.4 Reglas para la Multifirma en ADI

Una versión de un documento puede tener una o varias firmas, y éstas pueden ser paralelas o secuenciales, pero todas ellas deben residir en una sola estructura de firma.

En caso de que una versión de un documento tenga varias firmas, todas ellas deben ser del mismo tipo: todas attached o detached (y enveloped o enveloping si procede). Asimismo, todas deben tener el mismo formato y subformato: CAdES-BES, XAdES-EPES, etc.

El tratamiento de las firmas y la multifirma se describe con más detalle en el “Manual de Integración del Archivo Electrónico”.

6.1.5.5 Reglas comunes a tener en cuenta

Reglas de creación de firma para documentos electrónicos

El firmante debe asegurarse que no existen contenidos dinámicos (por ejemplo macros) en el fichero a firmar que pudiese modificar el resultado de la firma a lo largo del tiempo.

La vinculación del firmante se establecerá a través de etiquetas que, incluidas bajo la firma, y definidas según los estándares correspondientes proporcionarán la siguiente información:

- Fecha y hora de la firma
- Certificado del firmante
- Política de firma en que se basa el proceso de generación de firma.
- Formato del documento original, para que el receptor sepa como visualizar el documento.

Podrán agregarse, con carácter opcional, las siguientes etiquetas:

- Lugar geográfico donde se realiza la firma
- Rol del firmante
- Acción del firmante sobre el documento
- Sello de tiempo sobre todos o alguno de los objetos de la firma

Reglas de validación de firma electrónica

Independientemente del formato utilizado, para verificar la validez de la firma, el verificador podrá considerar la siguiente información:

- Fecha y hora de la firma. Se utilizará en la verificación de firmas para comprobar el estado de los certificados en la fecha señalada. Si se ha realizado sello de tiempo, la fecha de la firma se determina mediante el sello más antiguo dentro de la estructura de la firma. SigningTime (XAdES), Signing-time (CAdES)
- Certificado del firmante. Se utilizará para verificar el estado del certificado, y si fuera necesario, la cadena de certificación en la fecha de firma. SigningCertificate (XAdES), ESS signing-certificate o ESS signing-certificate v2 (CAdES)
- Política de firma. Permite comprobar que la política utilizada en la generación de firma se corresponde con la que debe usarse. La firma debe estar disponible en un formato interpretable (XML o ASN.1). SignaturePolicyIdentifier (XAdES), SignaturePolicyIdentifier (CAdES)

En el caso de que se hayan realizado varias firmas en el documento (el atributo CounterSignature informa sobre las firmas generadas) se verificarán todas las firmas del modo descrito.

Además de lo descrito en la política de firma, el verificador podrá definir sus procesos de validación y archivado según los requisitos de la política de firma particular a la que se ajusta el servicio.

Para comprobar el estado de revocación de un certificado hay que tener en cuenta el **periodo de precaución / periodo de gracia**. Este tiempo es la demora entre el instante en que el firmante inicia la revocación de un certificado hasta que se distribuye a los puntos de información. Se recomienda que este periodo sea como mínimo el tiempo máximo de refresco completo de las CRLs (Certificate Revocation List) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). El verificador puede esperar este tiempo para validar la firma o validarla en el mismo momento y revalidarla posteriormente.

6.1.5.6 Reglas de confianza

Reglas de confianza para los sellos de tiempo

El sello de tiempo nos indica la fecha y hora exacta en que se ha producido un acto, asegurando que tanto los datos que van a ser firmados como la información del estado de los certificados se generaron antes de un determinado instante. Para ello una Autoridad de Sellado de Tiempo (TSA) actúa como tercero de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

En el caso de documentos digitales la hora del archivo no es ninguna evidencia de la hora en que se firmó el documento; ni técnicamente se puede garantizar, ni tiene cobertura jurídica.

Los elementos básicos que componen un sello digital de tiempo son:

- **Datos sobre la identidad de la autoridad emisora** (identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, el algoritmo de firma digital y la función hash utilizados).
- **Tipo de solicitud cursada** (si es un valor hash o un documento, cuál es su valor y datos de referencia).
- **Parámetros del secuenciador** (valores hash "anterior", "actual" y "siguiente").
- **Fecha y hora UTC**.
- **Firma digital** de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo y la información de validación pueden ser añadidos por el emisor, el receptor o un tercero y se deben incluir como propiedades no firmadas en el campo SignatureTimeStamp (Signature-time-stamp para CAdES).

El sellado de tiempo debe realizarse en un momento próximo a la fecha incluida en el campo SigningTime (Signing-time para CAdES) y, en cualquier caso, siempre antes de la caducidad del certificado del firmante.

Reglas de confianza para firmas longevas

Las firmas longevas permiten garantizar su validez a largo plazo, una vez vencido el periodo de validez del certificado.

Los formatos XAdES y CAdES permiten incorporar información adicional, que puede ser incluida tanto por el firmante como por el verificador con el fin de garantizar la validez de la firma a lo largo del tiempo. Esta información se recomienda añadirla después de transcurrido el periodo de precaución o periodo de gracia. Para generar firmas longevas se recomienda incluir un sello de tiempo que permita garantizar que el certificado era válido cuando se realizó la firma.

Para convertir una firma electrónica a firma longeva deben darse las siguientes condiciones:

- Debe verificarse la firma electrónica validando la integridad de la firma, el cumplimiento de los estándares de firma y las referencias.
- Debe realizarse un completado de la firma electrónica, que consiste en:
  - Obtención de las referencias a los certificados, y almacenamiento de los certificados del firmante y de la cadena de certificación.
  - Obtención de las referencias a las informaciones de estado de los certificados (CRLs o las respuestas OCSP), y almacenarlas.
- Sellado de, al menos, referencias a los certificados y a las informaciones de estado.

Por tanto se incluirá información adicional de validación

- Información del estado del certificado en el momento en que se produce la validación de la firma o una referencia a los mismos.
- Certificados que conforman la cadena de confianza.

A partir del formato básico (BES) los formatos XAdES y CAdES permiten utilizar estructuras

para firmas longevas donde incluir información para validar la firma a largo plazo.

6.1.5.7 Archivado y custodia

El archivo y custodia de documentos debe garantizar la autenticidad e integridad de los documentos a lo largo del tiempo. En el mundo electrónico, a día de hoy, la única forma de asegurarlo es utilizando técnicas de firma digital:

- Deberá verificarse la integridad de la firma, lo que demuestra que el documento no se ha modificado desde su firma.
- Deberá verificarse la validez del certificado, lo que asegura la identidad del firmante.
- Deberá verificarse que el certificado no está revocado (mediante CRL u OCSP), lo que asegura la validez del certificado.

De esta forma, para documentos firmados electrónicamente, ADI se encargará de archivar los siguientes objetos:

- Los documentos electrónicos firmados
- Las firmas electrónicas asociadas a los documentos electrónicos.
- Los informes/respuestas de validez de dichas firmas obtenidos después de su verificación.

ADI almacenará automáticamente la fecha y hora en que guarda cada uno de estos elementos.

Para garantizar la custodia (integridad a largo plazo) de estos objetos, ADI utilizará la custodia de evidencias de la Plataforma de Firma Electrónica:

- ADI calculará varios hashes (evidencias) basados en distintos algoritmos, de cada objeto.
- Enviará esos resúmenes a la Plataforma de Firma Electrónica (PFE) para su custodia:
    - La PFE firma con certificado de Gobierno de Navarra y sello de tiempo las evidencias, generando una estructura XAdES-A.
    - Durante el tiempo que se le haya indicado
        - Continua resellando las evidencias (así el sello más externo siempre será válido)
        - Impide su borrado.

6.1.6 Representación e impresión de documentos electrónicos

La representación de los documentos electrónicos comprende la reproducción del contenido del documento y/o de sus metadatos y de las firmas electrónicas correspondientes.

Los documentos electrónicos deben ser reproducidos por las unidades administrativas que los gestionan en el ejercicio de sus funciones, pero además pueden ser puestos a disposición de los ciudadanos o de otras Administraciones por medio de la sede electrónica o los canales de comunicación que correspondan en cada caso.

La visualización de los documentos electrónicos puede, por tanto, comprender la representación de los siguientes componentes:

- Contenido del documento
- Firmas electrónicas
- Metadatos

Así mismo, la visualización o representación del documento electrónico puede conllevar la descarga del documento o su impresión.

Código de Verificación

La Ley Foral 11/2007 para la Implantación de la Administración Electrónica en la Administración de la Comunidad Foral autoriza el uso del Código de Verificación en la expedición de un certificado administrativo por medios electrónicos:

> *Los certificados administrativos por medios electrónicos producirán idénticos efectos a los expedidos en soporte papel. A tal efecto, su contenido deberá poder ser impreso en soporte papel, en el que la firma manuscrita será sustituida por un código de verificación generado electrónicamente que permita en su caso contrastar su autenticidad accediendo por medios telemáticos a los archivos del órgano u organismo emisor.*

Por otra parte, la ley 11/2007, de 22 de junio, de acceso de los ciudadanos a los servicios públicos, indica en el artículo 30.5:

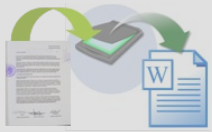
> *Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tienen la consideración de copias autenticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan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

ADI proporcionará servicios relativos al Código de Verificación, permitiendo que se incluya como uno de los metadatos del documento electrónico, así como la recuperación y consulta del documento a partir de su Código.

6.1.7 Copiado y conversión de documentos

6.1.7.1 Originales y copias de documentos: conceptos

Un documento **original** es aquel que se conserva tal y como fue emitido por su autor, tanto en sus caracteres externos como internos.



Una **copia** es el resultado de la reproducción de un documento.

Desde el punto de vista legal hay dos tipos de copia: la **copia simple**, aquella que no tiene ni valoraciones ni suscripciones, y la **copia auténtica**, aquella que tiene un valor probatorio dado por la autoridad de la persona que la realiza.

La NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos es la norma que ha establecido con más detalle las condiciones para la obtención de copias electrónicas auténticas.

En esta NTI se establece, entre otras condiciones, que las copias auténticas se expedirán a partir de documentos con calidad de original o copia auténtica y que serán firmadas mediante alguno de los sistemas de firma previstos en los artículos 18 ó 19 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.

En el caso de copias auténticas en papel de documentos electrónicos, la NTI solo establece las condiciones para aquellas cuyo documento origen es un documento público administrativo.

Según el artículo 1216 del Código Civil, Son documentos públicos los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley. Por otro lado, en el artículo 46-4 de la ley 30/1992 de Régimen Jurídico de las Administraciones publicas y del Procedimiento Administrativo Común, se definen como los válidamente emitidos por los órganos de las Administraciones Públicas.

6.1.7.2 Escenarios de copiado de documentos

Registro Electrónico

Por medio del Registro Electrónico pueden añadirse a una solicitud diferentes adjuntos que, en origen, pueden ser originales, copias simples o copias auténticas, públicos o privados, según la documentación que se solicite en cada procedimiento.

En la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos, (art. 35) se refieren a estos adjuntos como ***copias digitalizadas***:

Los interesados podrán aportar al expediente copias digitalizadas de los documentos, cuya fidelidad con el original garantizarán mediante la utilización de firma electrónica avanzada.

La Administración Pública podrá solicitar del correspondiente archivo el cotejo del contenido de las copias aportadas. Ante la imposibilidad de este cotejo y con carácter excepcional, podrá requerir al particular la exhibición del documento o de la información original.

Registro Presencial

En el registro presencial los ciudadanos pueden aportar originales, copias simples o copias auténticas, públicos o privados, según la documentación que se solicite en cada procedimiento. En este escenario se utilizará el método definido en ADI para la "digitalización certificada" y que tendrá como objetivo la obtención de **copias electrónicas de documentos en papel**.

Tramitación

Los documentos electrónicos originalmente emitidos por la Administración de la Comunidad Foral durante la tramitación tendrán la consideración de **originales**.

6.1.7.3 Conversión de documentos administrativos

Habitualmente las unidades administrativas trabajan con diferentes formatos de documentos y realizan una conversión a PDF antes de su firma definitiva y su archivado.

Adicionalmente, al dar de alta un documento en el Archivo Digital, podrá solicitarse su conversión a PDF/A.

Para realizar la conversión a PDF/A hay que tener en cuenta que el documento a convertir debe ser un documento "original" y "preliminar" y no debe estar firmado previamente.

Una vez se realice la conversión a PDF/A y la/s firma/s del documento, éste podrá obtener la condición de documento "original" y "final"

6.1.7.4 Copiado de documentos

Esta utilidad del Archivo Digital permite la copia de un documento con la finalidad de incluirlo en otro expediente o para su remisión a otra administración. Se realizará una copia idéntica, tanto del contenido del documento como de sus metadatos y firmas. Solamente podrán ser copiados los documentos "finales".

6.1.7.5 Conversión de formatos obsoletos

ADI cuenta con un servicio específico para la conversión de formatos obsoletos.

Este servicio permite guardar tanto los ficheros en el nuevo formato como el formato más antiguo o el original.

Los motivos para almacenar el fichero origen junto al nuevo formato convertido son los siguientes:

- Las sucesivas migraciones pueden dar lugar a pérdidas de información. En ciertos casos puede ser conveniente realizar una conversión de formato a partir del documento original, en lugar de utilizar su copia.
- La conservación del formato antiguo u original demuestra y traza el nivel de pérdida de información en el formato migrado.

Si en un futuro se decide que la eliminación del formato antiguo/original, los documentos se deberán destruir siempre con la autorización específica de la Comisión de Evaluación Documental.

Las fases de preparación del proceso de conversión y validación se describen en el apartado *Proceso de conversión de formatos obsoletos*.

6.1.8 Digitalización

La digitalización de documentos en papel tiene grandes beneficios: permite gestionar los documentos con mayor eficiencia y permite generar expedientes electrónicos completos, eliminando el complejo control de los expedientes mixtos (expedientes que contienen documentos en papel y en electrónico).

Diferentes departamentos de Gobierno de Navarra han realizado digitalizaciones de sus documentos administrativos con la finalidad consultarlos de forma más rápida. Las imágenes obtenidas de esta forma no sustituyen al documento original digitalizado, que posee todo su valor probatorio y debe ser conservado en su soporte papel.

Gobierno de Navarra va a establecer una política de digitalización, apoyada en una legislación específica y que permita la obtención de copias electrónicas de documentos con la misma validez que los documentos en soporte papel.

Esta voluntad está amparada en la legalidad vigente. Los principios aportados por la Ley 30/1992 en cuanto a validez y eficacia de documentos y copias, fueron desarrollados en la Ley 11/2007, que en su artículo 30 permite la copia electrónica de los documentos en papel:

> *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.*
>
> *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.*

6.1.8.1 Procedimiento para la obtención válida de copias electrónicas de documentos en papel

El procedimiento de digitalización permitirá la obtención de copias fieles e íntegras de documentos en papel presentados por los ciudadanos en los procedimientos administrativos o generados por Gobierno de Navarra durante su tramitación.

El proceso de digitalización estará diseñado de manera que garantice que no se han producido alteraciones en el documento desde el momento de obtención de la imagen digitalizada.

El resultado del proceso de digitalización segura será una imagen fiel e íntegra del documento digitalizado, firmada electrónicamente y descrita mediante los metadatos requeridos.

La integridad y conservación de las imágenes resultantes quedarán garantizadas por su almacenamiento en ADI.

Los requerimientos técnicos (formatos, resolución…), así como las pautas que deben seguirse, estarán disponibles en la web de Gobierno de Navarra.

6.1.8.2 Determinación de órganos competentes para realizar las copias

El artículo 46.1 de la Ley 30/1992 establece que cada Administración Pública determinará reglamentariamente los órganos que tengan atribuidas las competencias de expedición de copias auténticas de documentos públicos o privados.

En la Administración de la Comunidad Foral las indicaciones sobre la competencia al respecto se encuentran en diferentes regulaciones:

- Las Secretarías Generales Técnicas tienen competencia para dar fe y librar las oportunas certificaciones de las órdenes forales de los Consejeros, de las resoluciones de las unidades orgánicas del respectivo Departamento, así como de documentos y datos que obren en el Departamento (Decreto Foral 29/2005)
- Registro General y Registros auxiliares tienen entre sus funciones la "autenticación de copias de documentos privados y compulsa de documentos públicos" (Decreto Foral 137/2002)

Según establece la Orden Foral 164/1994, la autenticación se realizará mediante la estampación, en cada documento, de un sello en el que conste su correspondencia con el documento original exhibido, el órgano que lo acredita y la firma del funcionario que materializa la autenticación.

Los ciudadanos, en sus relaciones con las Administraciones Públicas tienen derecho a obtener copia sellada de los documentos que presenten, aportándola junto con los originales, así como a la devolución de éstos, salvo cuando los originales deban obrar en el procedimiento. Cuando el original deba obrar en el procedimiento, se entregará al ciudadano la copia del mismo, una vez sellada por los registros y previa comprobación de su identidad con el original (Ley 30/1992).

- Los funcionarios responsables del archivo podrán emitir y transmitir por medios electrónicos copias compulsadas de los documentos originales que obren en el mismo (Ley Foral 11/2007).
- Los documentos electrónicos o copias de ellos emitidos por los órganos de la Hacienda Tributaria de Navarra, que hayan sido generados por medios electrónicos, informáticos y telemáticos, serán válidos siempre que se garantice su autenticidad, integridad y conservación.

Las copias de los documentos originales que realice la Hacienda Tributaria de Navarra para su conservación o tratamiento en formato electrónico tendrán la misma validez y eficacia que los documentos originales siempre que quede garantizada su autenticidad, integridad y conservación (Decreto Foral 50/2006)

6.2 Competencias y responsabilidades

En este apartado se especifican las áreas de competencia y responsabilidades en materia de gestión de documentación electrónica de archivo.

Estas competencias y responsabilidades son asumidas y ejercidas por estructuras organizativas del Gobierno de Navarra, coordinadas desde una Unidad que vela por la aplicación del Modelo.

Con base en las actuales estructuras responsables, se establece la estrategia organizativa necesaria para llevar a cabo el despliegue en las diferentes unidades y aplicaciones. Para este despliegue se requieren actividades organizativas, funcionales de archivística y gestión documental, jurídicas y tecnológicas.

Por tanto la nueva estrategia organizativa debe tener un **carácter multidisciplinar** y contemplar responsabilidades a diferentes niveles, siendo la propuesta inicial el siguiente modelo organizativo:

- **Comisión Estratégica del Sistema de Gestión Documental de Navarra (ADI-E).**

  Encargada de marcar o revisar los objetivos del sistema de gestión documental, realizar el seguimiento del cumplimiento de los mismos, así como de encargar al Equipo Operativo el cumplimiento de las decisiones estratégicas que tome la Comisión y de recibir y estudiar las solicitudes elevadas a ella desde el Equipo Operativo.

  Estará formada por:

  - Responsable de las funciones de gestión documental y archivística.
  - Un representante de la Comisión de Evaluación Documental.
  - Responsable de las funciones de organización.
  - Responsable de las funciones de tecnología.
  - Responsable de las funciones de acción legislativa.

- **Equipo Operativo de Trabajo para Sistema de Archivo Digital (ADI-O):**

  Encargado de ejecutar las decisiones tomadas por ADI-E, de velar por el correcto funcionamiento del sistema y elevar a ADI-E aquellas decisiones que estime oportuno.

  Se apoya en los grupos ya existentes para realizar su labor.

  Deberá estar integrado por, al menos, una persona de cada uno de estos perfiles:

  - Gestión documental y archivo
  - Tecnológico/informático
  - Organizativo
  - Normativo-legislativo
  - Seguridad

- **Responsable Técnico (ADI-RTec).**

  Persona del área tecnológica que vela por el cumplimiento global del nivel de servicio de ADI, promoviendo las acciones y proyectos de mejora oportunos.

- **Responsable de Explotación (ADI-RExpl).**

  Persona del área tecnológica que se encarga, mediante la adecuada coordinación de los técnicos disponibles, de proporcionar el nivel de servicio de las infraestructuras y de ADI.

6.2.1 Funciones

A continuación se describe cada una de las funciones:

6.2.1.1 Impulso y coordinación del Modelo y Plan de despliegue

Definición de la estrategia de despliegue, así como la responsabilidad de la toma de decisiones estratégicas y gestionar las directrices, los objetivos y el alcance del Modelo y Plan de despliegue.

6.2.1.2 Promoción y difusión

Promoción y difusión del sistema, tanto internamente a los Departamentos y organismos dependientes del Gobierno de Navarra como externamente.

6.2.1.3 Definición y mantenimiento de herramientas de organización documental

- Control del catálogo de procedimientos y series documentales del Gobierno de Navarra.
- Gestión y el mantenimiento del cuadro de clasificación
- Equivalencia y coordinación de la definición de los procedimientos y el cuadro de clasificación

- Evaluación documental de las series documentales/procedimientos
- Participación en la creación de nuevos procedimientos y series documentales.
- Control y mantenimiento de las tipologías documentales
- Control y mantenimiento de las entidades y metadatos del sistema
- Control y mantenimiento de otras posibles reglas de gestión asociadas a los documentos electrónicos

6.2.1.4 Definición y mantenimiento de políticas y recomendaciones

Las políticas y recomendaciones definidas en el presente Modelo habrán de ser actualizadas en la medida que evolucione la normativa y legislación que afecte al sistema, la infraestructura y tecnologías que lo soportan.

6.2.1.5 Mantenimiento y actualización del Modelo de Gestión Documental

El presente Modelo de Gestión Documental deberá mantenerse actualizado integrando información pertinente que resulte de:

- Los estudios que se vayan realizando
- La incorporación de nuevos requisitos y funcionalidades al sistema
- Los posibles cambios en la infraestructura técnica
- La integración de sistemas con el sistema de gestión documental con ADI
- La documentación divulgativa resultante de las actividades de difusión
- Las nuevas responsabilidades que puedan definirse
- La incorporación y adecuación del sistema a la nueva normativa y legislación que le afecte, etc.

6.2.1.6 Vigilancia y seguimiento de normativas y legislación externas que afecten al sistema

Puede que sea necesario modificar o elaborar nueva normativa y legislación que no sólo contemple el archivo físico, sino también la gestión de los documentos administrativos electrónicos y ADI.

6.2.1.7 Formación y transmisión de conocimiento en procesos operativos de gestión documental y administración electrónica

Será necesario formar a personal con responsabilidad en la producción administrativa para la adquisición de conocimiento especializado. Esta formación les capacitará para optimizar su respuesta en la realización de procesos operativos relativos a la gestión de documentos electrónicos.

6.2.1.8 Análisis de necesidades y adquisición de nuevo equipamiento informático hardware y software base

Analizar las necesidades técnicas en cuanto a infraestructura de hardware necesaria para el óptimo funcionamiento y rendimiento del sistema y del software, sobre todo antes de la incorporación de aplicaciones en la que se prevea un aumento importante de la carga del sistema.

6.2.1.9 Desarrollo de la integración de los sistemas corporativos o departamentales con el sistema

Coordinación del desarrollo, las pruebas y la implantación y puesta en marcha de la integración de los sistemas corporativos con el sistema según el modelo de gestión documental, las especificaciones técnicas de integración definidas y el análisis de integración realizado.

6.2.1.10 Configuración y administración del sistema.

6.2.1.11 Gestión de nuevas funcionalidades y prestaciones:

- La identificación nuevos requisitos y necesidades documentales.
- El análisis de los requisitos detectados y su impacto en el sistema (metadatos, asociaciones, firmas,…).
- La adaptación del sistema a las nuevas exigencias.

6.2.1.12 Mantenimiento de la infraestructura tecnológica del sistema.

Proporcionar el nivel de servicio de las infraestructuras y sistemas de información implantados solicitado por la Comisión Estratégica coordinando los técnicos y medios disponibles.

6.2.1.13 Soporte funcional y técnico del sistema

6.2.1.14 Mantenimiento perfectivo del sistema.

Ampliación, rediseño y perfeccionamiento del sistema, con el objetivo de aumentar los niveles de calidad del sistema.

6.2.1.15 Mantenimiento correctivo del sistema.

6.2.2 Responsabilidades

En esta matriz RACI se indican las responsabilidades de las funciones enumeradas anteriormente:

Función	ADI-E	ADI-O	CED	RTec	RExpl
Impulso y coordinación del Modelo y Plan de despliegue	A	R	C		
Promoción y difusión	A	R	C		
Definición y mantenimiento de herramientas de organización documental	A	R	I	C	
Definición y mantenimiento de políticas y recomendaciones	A	R	I	C	C
Mantenimiento y actualización del Modelo de Gestión Documental	A	R	I	C	C
Vigilancia y seguimiento de normativas y legislación externas que afecten al sistema	A	R	I		
Formación y transmisión de conocimiento en procesos operativos de gestión documental y administración electrónica	A	R			
Análisis de necesidades y adquisición de nuevo equipamiento informático hardware y software base		A		R	C
Desarrollo de la integración de los sistemas corporativos o departamentales con el sistema		A		R	C
Configuración y administración del sistema.		A		R	
Gestión de nuevas funcionalidades y prestaciones		A		R	C
Mantenimiento de la infraestructura tecnológica del sistema		A			R
Soporte funcional y técnico del sistema		A		R	C
Mantenimiento perfectivo del sistema				A	R
Mantenimiento correctivo del sistema				A	R

- **R** (Responsible / Responsable): realiza el trabajo y es responsable por su realización. Es quien debe ejecutar las tareas.
- **A** (Accountable / Aprobador): se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Es quien debe asegurar que se ejecutan las tareas.
- **C** (Consulted / Consultado): posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
- **I** (Informed / Informado): Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

6.3 Metadatos

La consecución de una correcta gestión documental implica adquirir un compromiso entre los dos aspectos siguientes:

- Definir un conjunto de metadatos que permita el rápido acceso y gestión de los documentos por parte de distintos sistemas de información.
- No sobrecargar la tarea de categorización de documentos, de forma que no se vea afectada la tarea administrativa.

Inicialmente, los metadatos definen el documento en el mismo momento de su incorporación, situándolo en su contexto y estableciendo una identificación para su gestión.

6.3.1 Esquema de metadatos

El esquema de metadatos refleja los metadatos que deberán incorporarse a documentos, expedientes (clasificados en sus correspondientes procedimientos administrativos) y firmas electrónicas.

Para facilitar la compresión de la implementación de los metadatos se han subdividido en:

- Metadatos descriptivos: deben ser completados por las aplicaciones de registro y tramitación. Tienen como objetivo la descripción e identificación de documentos y expedientes, así como sus condiciones de acceso.
- Metadatos del ciclo de vida: dependen del ciclo de vida del documento y se completan a partir de acciones realizadas en las aplicaciones de registro/tramitación/archivo
- Metadatos administrativos y técnicos: completados por la plataforma ADI durante la captura y gestión de los documentos o bien en la configuración de la plataforma.
- Metadatos de seguridad: completados por las aplicaciones de registro/tramitación/archivo
- Metadatos de firma: incorporados a ADI por las aplicaciones de registro/tramitación a partir de la información proporcionada por la Plataforma de Firma Electrónica.

Obligatoriedad en la cumplimentación de los metadatos

En las tablas siguientes, la columna Oblig. Indica la obligatoriedad de cumplimentar el metadato por parte de las aplicaciones que guardan los documentos en ADI, los valores posibles son:

- **No**: opcional.
- **Sí***: Obligatorio tanto para documentos y expedientes pertenecientes a un procedimiento administrativo en fase de tramitación (expedientes abiertos), como para documentos y expedientes pertenecientes a un procedimiento administrativo en fase activa, semiactiva o histórica (expedientes cerrados).
- **Sí****: Obligatorio para documentos y expedientes pertenecientes a un procedimiento administrativo en fase activa, semiactiva o histórica (expedientes cerrados).
- **Adi**: Los asigna ADI automáticamente.

6.3.1.1 Metadatos descriptivos para DOCUMENTO

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
FechaAdministrativa	Referencia temporal administrativa	Date	Sí*	Dependiendo del tipo de documento: en una solicitud es la fecha de presentación en Registro, en una	S	N

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
				resolución la fecha en que se firma… etc Formato: AAAA-MM-DD		
OrigenCiudadanoAdministracion	Indica si el documento proviene de un ciudadano, de otra Administración o ha sido generado por unidad administrativa de Gobierno de Navarra	Integer	No	0: Ciudadano 1: Administración 3: Gobierno de Navarra	S	N
Órgano	Código del productor (unidad de Gobierno de Navarra responsable de captura)	Text	Si*	Codificación de organismos de Gobierno de Navarra (mantenida por Función Pública)	S	N
Titulo	Titulo del documento que se mostrará en las consultas	String	Si*	Titulo del documento	S	N
TipoDocumento	Tipo de documento: resolución, factura, solicitud…	Text	Si*	Según la lista de valores de tipo de documento	S	N
Idioma	Idioma(s) del documento	Text	No	Lista de valores según la norma ISO 639-1	S	S
Descripcion	Descripción detallada/ampliada del documento	Memo	No	Texto libre que describe el contenido	S	N
NivelLOPD	Nivel básico, medio o alto según la Ley de Protección de datos personales	Integer	Sí*	0: No aplica 1: Básico 2: Medio 3: Alto	S	N
Acceso	Señala si se usará la cuenta pública o privada	Integer	Sí*	1: Público 2: Privado	N	N

6.3.1.2 Metadatos del ciclo de vida para DOCUMENTO

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
GradoDocumental	Indica si el documento es final o preliminar	Integer	Si*	1: Preliminar 2: Final	S	N
EstadoElaboracion	Indica si el documento es original o copia	Text	Si*	EE01: Original EE50: Copia simple EE51: Copia electrónica compulsada	N	N
Conservación	Indica si el documento es de conservación permanente o si se puede eliminar pasado un plazo determinado	Text	Sí**	S: Conservación N: Eliminación	S	N

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
Plazo	Si el metadato *Conservación* está a *N*. Se indica el plazo (en años) a partir del cual se puede eliminar	Integer	SÍ**	Valor > 0	S	N
IdentificadorDocumentoOrigen	Identificador del documento origen en caso de que el estado de elaboración sea una copia (EE02, EE03)	String	No	Identificador documento en UCM	N	N
OrganismoExpideCopia	Organismo de Gobierno de Navarra que genera la copia mediante el servicio del framework habilitado para ello	Text	No	Codificación de organismos de Gobierno de Navarra	N	N
FechaExpideCopia	Fecha de expedición de la copia	Date	No	Formato AAAA-MM-DD	N	N
Ciclovida	Subsistema de nivel de Archivo	String	Adi	Archivo_Gestión_Registro Archivo_Gestión_Tramitación Archivo_Administración Archivo_General	S	N

6.3.1.3 Metadatos administrativos para DOCUMENTO

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
DocType	Tipo del objeto en UCM	String	Adi	Documento	N	N
Identificador	Identificador en UCM (dDocName)	String	Adi	Asignado automáticamente por UCM	N	N
CVE	Código de verificación	Long Text	No	Según decisión sobre composición del CVE en Gobierno de Navarra	N	N
AplicacionOrigen	Aplicación desde la que se inserta el documento en UCM	Text	Sí*	Identificador de la aplicación que almacena el documento. Se asigna al solicitar la integración en ADI.	N	N
FamiliaDocumental	Familia documental a la que pertenece el documento	Text	Adi	Lo asigna automáticamente UCM en función del tipo documental	S	N

6.3.1.4 Metadatos seguridad para DOCUMENTO

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
DSecurityGroup	Grupo de seguridad en UCM al que se asignan los documentos para	String	Adi	Grupos de Seguridad creados en UCM. Lo asigna	S	N

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
	control de accesos			automáticamente ADI		
CuentaSeguridad	Cuenta de seguridad que da acceso al documento en combinación con el DSecurityGroup	String	Adi	Cuentas de seguridad creadas en UCM. La asigna automáticamente ADI	S	N

6.3.1.5 Metadatos de firma para DOCUMENTO*

Un documento puede tener asociadas varias firmas electrónicas, por lo que el bloque de metadatos propuesto se aplica al objeto “firma” almacenado en ADI.

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
Firmado	Informa si el documento está firmado electrónicamente	Integer	Sí*	1: Sí 2: No 3: No comprobable	S	N
Firmante	Nombre o razón social del firmante	String	Si*, si firmado = 1	Persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa	N	N
Fechayhora	Fecha y hora de la firma	DateTime	Si*, si firmado = 1	Formato: AAAA-MM-DDTHH:MM:SS.mm (ISO 8601)	N	N
TipoFirma	Tipo de firma	Text	Si*, si firmado = 1	TF02: XAdEs Internally detached signature TF03: XAdEs enveloped signature TF04: CAdES detached/explicit signature TF05: CAdES attached/implicit signature TF06: PadES TF06: XAdEs Externally detached TF50: PDF Signature	N	N
Validadaenfecha	Fecha y hora en que la firma ha sido validada por SIAVAL o por otra plataforma de firma al efecto	DateTime	Si*, si firmado = 1	Formato: AAAA-MM-DDTHH:MM:SS.mm (ISO 8601)	N	N

*Además de estos metadatos almacenados en ADI y referentes a la firma, la plataforma de firma consigna en su sistema datos adicionales sobre la verificación y validación de la firma.

6.3.1.6 Metadatos Administrativos para Firma:

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
DocType	Tipo del objeto en UCM	String	Adi	Firma	N	N
Identificador	Identificador en UCM de las firmas electrónicas asociadas a documentos	String	Adi	Asignado automáticamente por UCM	N	N

6.3.1.7 Metadatos descriptivos para EXPEDIENTE

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
FechaAperturaExpediente	Fecha de apertura del expediente	Date	Si*	Formato: AAAA-MM-DD	N	N
FechaCierreExpediente	Fecha en la que la unidad tramitadora cierra el expediente	Date	Sí**	Formato: AAAA-MM-DD	N	N
Clasificacion	Código de procedimiento administrativo al que pertenece el Expediente	String	Sí**	Este metadato se completa de forma obligatoria en el momento de apertura del expediente. La lista de posibles procedimientos se asignará al solicitar la integración en ADI, ya que implica que el procedimiento administrativo tiene que estar evaluado documentalmente.	S	N
Titulo	Denominación (asunto) del expediente	String	Si**	Asunto del expediente. Normalmente será la denominación del procedimiento administrativo	S	N
NumExped	Número de Expediente	Text	No	Número de expediente en la aplicación tramitadora	S	N
InteresadoIdentidad	Nombre o razón social del interesado	Memo	Sí**	Apellidos, nombre de los interesados	S	S
Interesado NumIdentificación	Número de Identificación del interesado	Memo	Sí**	NIF, CIF…	S	S
Interesado Rol	Rol del interesado en el asunto: denunciante, promotor…	Memo	Sí**	Rol del interesado en el expediente	S	S
Organo	Código del productor (unidad de Gobierno de Navarra responsable de captura del expediente)	Text	Sí*	Codificación de organismos de Gobierno de Navarra	N	N
Descripcion	Descripción detallada/ampliada del expediente	Memo	No	Texto libre que describe el contenido	S	N

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
ExpedientesRelacionados	Expedientes que tienen alguna relación: por ejemplo un expediente de recurso administrativo estaría relacionado con el expediente que ha dado origen a dicho recurso	Memo	No	Números de los expedientes relacionados, según codificación de la aplicación de tramitación del expediente	S	S

*El número de expediente sí que es obligatorio para todas las aplicaciones de gestión que lo hayan consignado y puedan aportar ese dato a ADI

6.3.1.8 Metadatos del ciclo de vida para EXPEDIENTE

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
Estado	Indica el estado de elaboración del expediente	Text	Si*	E01 - Abierto E02 - Cerrado	N	N
Ciclovida	Subsistema de nivel de Archivo	String	Adi	Archivo_Gestión_Tramitación Archivo_Administración Archivo_Real_General	S	N
FechaArchivoAdministración	Fecha de traspaso al Archivo Administrativo del expediente	String	Adi	El valor se calcula a partir de la fecha de cierre del expediente	N	N

6.3.1.9 Metadatos administrativos para EXPEDIENTE

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
DocType	Tipo del objeto en UCM	String	Adi	Expediente	N	N
Identificador	Identificador en UCM	String	Adi	Lo asigna automáticamente UCM	N	N
AplicacionOrigen	Aplicación desde la que se crea el expediente en UCM	Text	Sí*	Identificador de la aplicación que almacena el documento. Se asigna al solicitar la integración en ADI.	N	N

6.3.1.10 Metadatos seguridad para EXPEDIENTE

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
DSecurityGroup	Grupo de seguridad en UCM al que pertenece el expediente. Este campo delimita los accesos al mismo.	String	Aut	Grupos de Seguridad creados en UCM. Lo asigna automáticamente ADI	S	N
CuentaSeguridad	Cuenta de seguridad que da acceso al documento	Strng	Aut	Cuentas de Seguridad creadas	S	N

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
	en combinación con el DSecurityGroup			en UCM. La asigna automáticamente ADI		

6.3.1.11 Otros metadatos para la gestión en ADI

Metadatos administrativos para PROCEDIMIENTO*

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
DocType	Tipo del objeto en ADI	String	Sí*	Procedimiento / Serie	N	N
Identificador	Identificador en ADI	String	Adi	Lo asigna automáticamente el sistema	N	N
CódigoProcedimiento	Identificador del procedimiento	String	Sí*	Catálogo de procedimientos de Gobierno de Navarra	S	N
CódigoSerieDocumental	Código de serie documental correspondiente	Text	Sí*	Cuadro de clasificación de Archivo Administrativo	S	N
Objeto	Finalidad y objeto del procedimiento administrativo	String	Sí*	Por ejemplo: “Aprobación y modificación de precios de servicio del transporte urbano”	S	N
Tramitacion	Tramitación que se sigue en ese procedimiento	String	Sí*	Por ejemplo: “las empresas concesionarias solicitan la revisión presentando una instancia a la que se adjunta un estudio económico…”	S	N
Legislacion	Legislación que afecta al procedimiento	String	Sí*	Por ejemplo: “Real Decreto 2695 sobre Normativa en materia de Precios. Ley 26/1984 para la defensa de los Consumidores…”	S	N
Documentosbasicos	Documentos básicos en ese procedimiento	String	Sí*	Por ejemplo: “Solicitud normalizada. Resolución…”	S	N

*Debe establecerse la correspondencia entre procedimientos y series documentales.

Metadatos administrativos de los ficheros almacenados en ADI

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
FormatoFic	Formato del fichero de	String	Adi	Seleccionable del	N	N

Metadato	Descripción	Tipo Dato	Oblig.	Valores	Modif.	Multivalor
hero	contenido. Atributo ya existente en el modelo propio de ADI			catálogo de formatos admitidos		
TamañoFichero	Tamaño del Fichero de contenido. Atributo ya existente en el modelo propio de ADI	String	Adi	Tamaño en bytes	N	N
ValorHuella	Huella del fichero	String	Adi	SHA-1#HASH_ADI#<has SHA-1>;SHA-256#HASH_ADI#<hash SHA-256>;MD5#HASH_ADI#<hash MD5>;RIPEMD160#HASH_ADI#<hash RIPEMD-160>	N	N

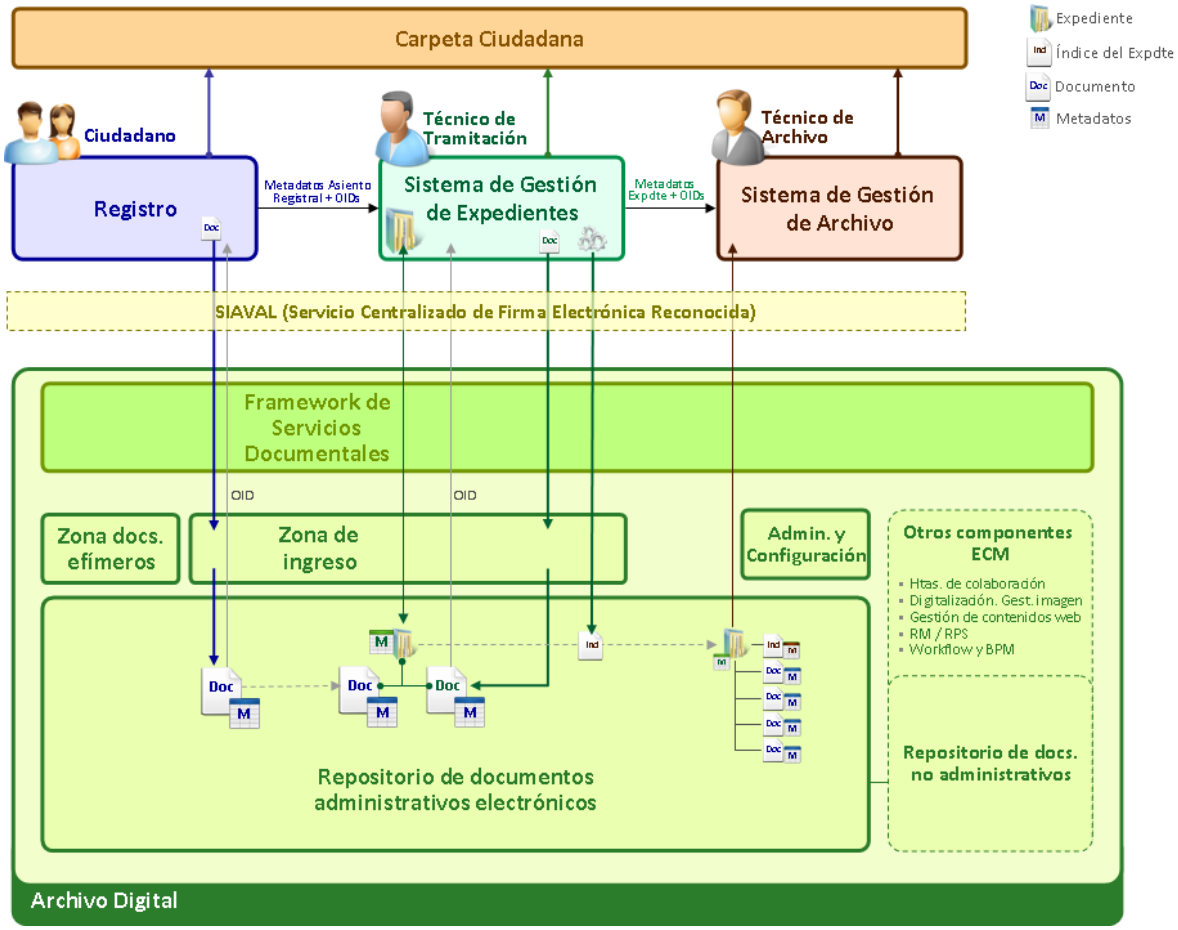
6.4 Definición de infraestructura técnica

En este apartado se presenta y define la infraestructura de ADI.

El sistema propuesto se compone, conceptualmente, de los siguientes elementos:

- Repositorio de documentos administrativos electrónicos
- Zona de ingreso
- Zona de documentos efímeros
- Repositorio de documentos no administrativos
- Administración y configuración
- Framework de servicios de gestión documental

Esta infraestructura deberá ser utilizada por los distintos sistemas/aplicaciones que gestionen documentos administrativos electrónicos. Los sistemas de Registro, Gestión de Expedientes y Gestión de Archivo deberán utilizar esta infraestructura para la gestión de sus documentos electrónicos.

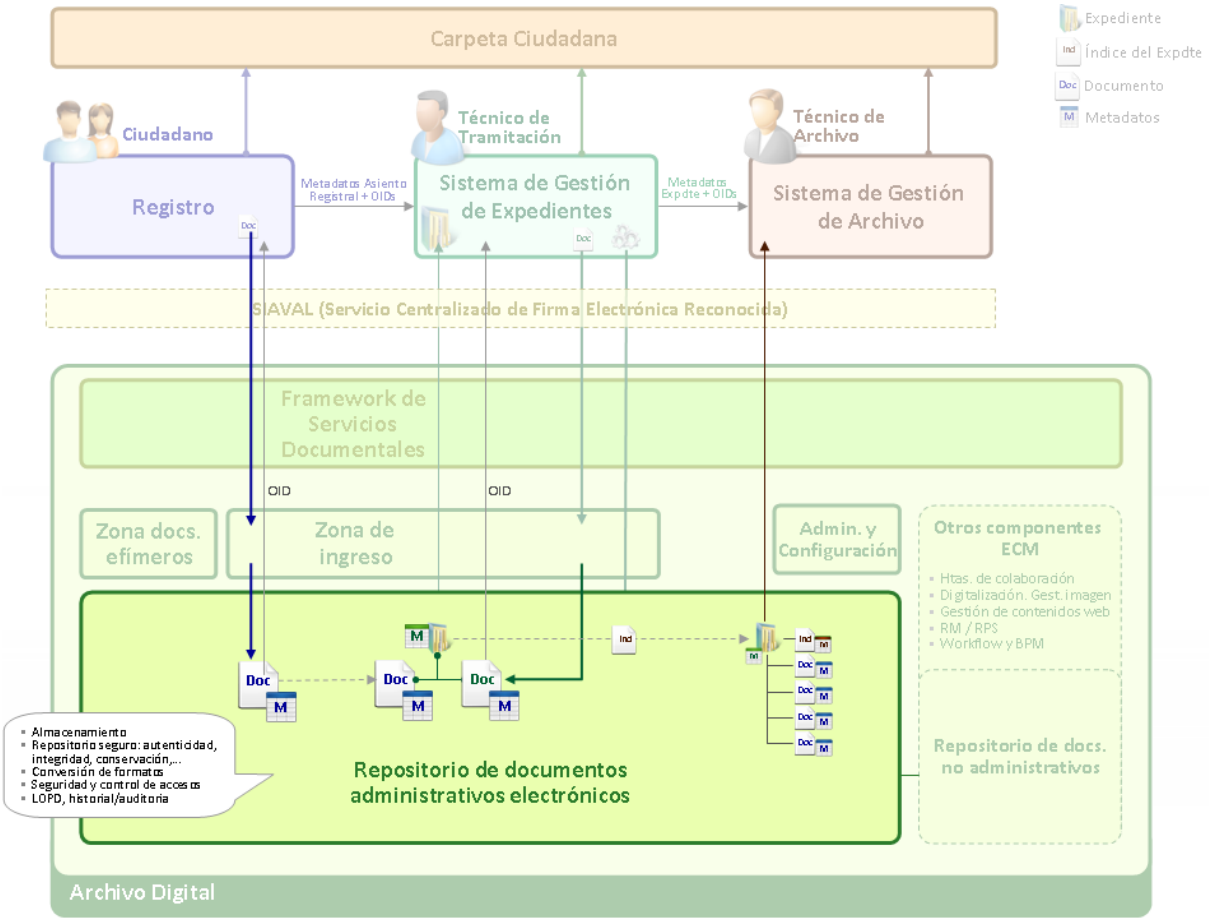


6.4.1 Repositorio de documentos administrativos electrónicos

6.4.1.1 Requisitos y Funcionalidades

El Repositorio de documentos administrativos electrónicos gestiona los documentos electrónicos, sus firmas y los metadatos, guardados con criterios de archivo, y gestionables mediante servicios web (a través del framework de servicios documentales).

Este repositorio da servicio a todos los procesos administrativos que requieran de gestión documental.



El repositorio de documentos administrativos electrónicos deberá mantenerse óptimamente organizado. Por ello todos los documentos que se incorporen deberán cumplir unos requisitos obligatorios y tener el conjunto exigido de metadatos que los identifiquen, describan y clasifiquen.

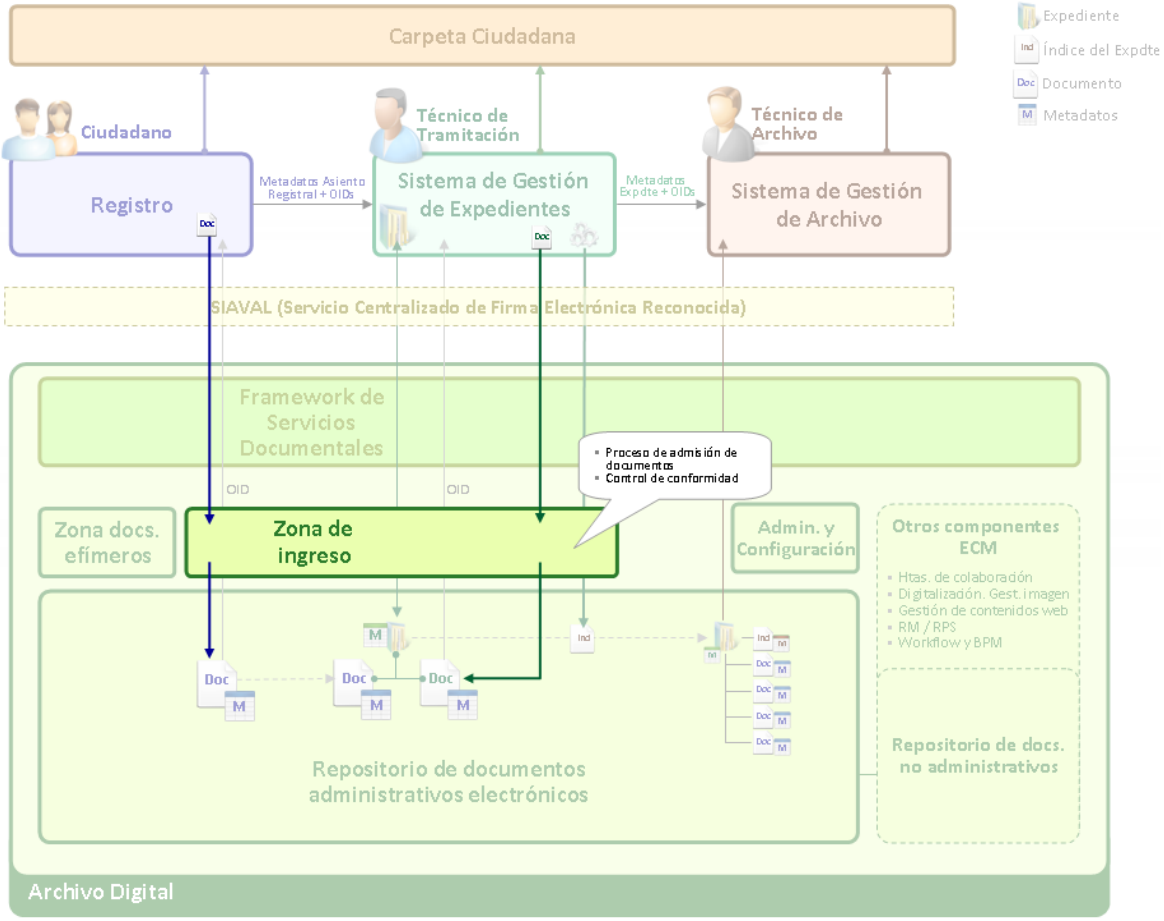
ADI asignará a cada documento que almacena un identificador único. La comunicación entre ADI y los sistemas/aplicaciones que harán uso de sus servicios, se realizará normalmente a través de los Identificadores.

Será obligatorio incorporar a este repositorio todos los documentos administrativos electrónicos que formen parte de los procedimientos administrativos. Estos documentos pertenecerán a un procedimiento/serie documental y serán tipificados según una tipología documental.

6.4.2 Zona de ingreso

Este módulo se encargará de realizar un control de conformidad para todos los documentos que ingresen en ADI y que implica los siguientes procesos:

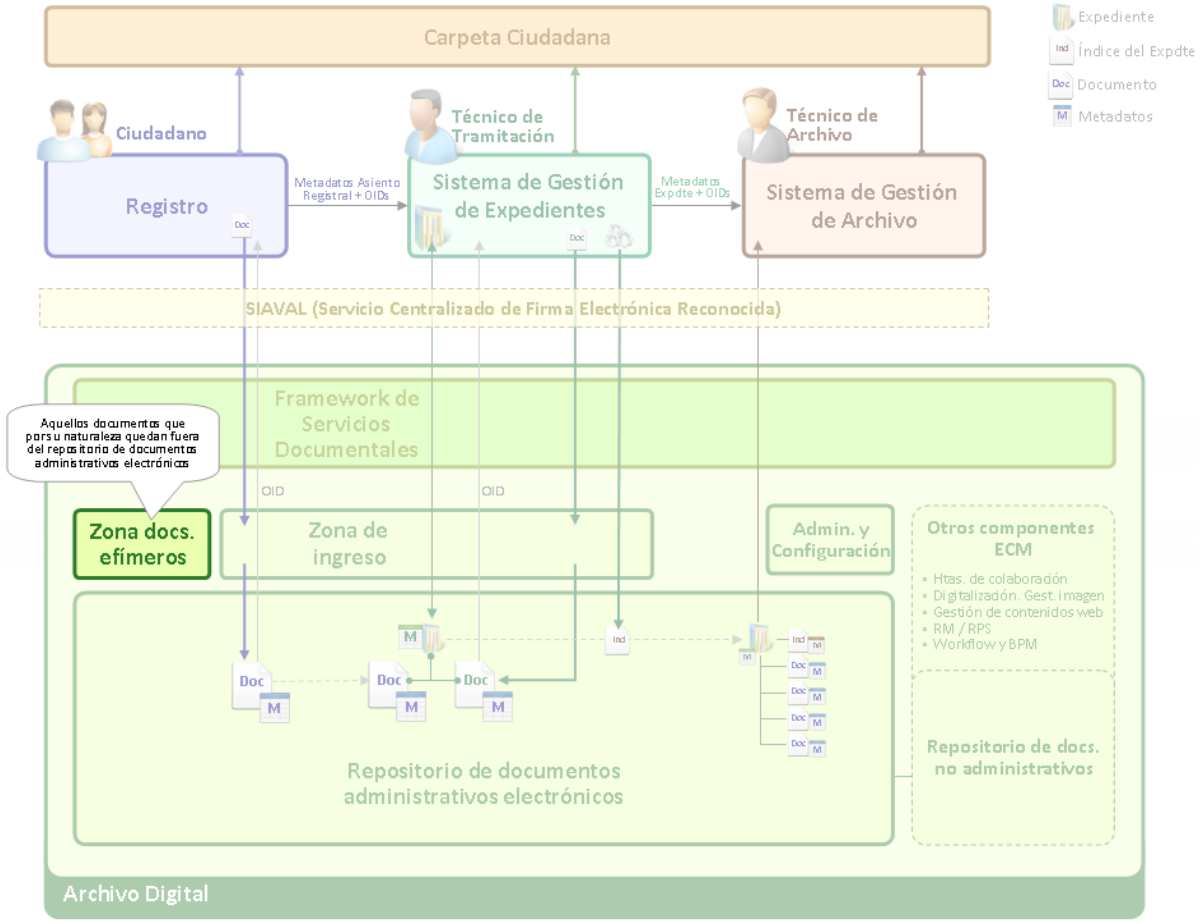
- Comprobar que el formato del fichero es uno de los admitidos en el sistema.
- Comprobar que el documento contiene información en los metadatos obligatorios



6.4.3 Zona de documentos efímeros

El objeto de esta zona es que los documentos no se queden en ella indefinidamente, principalmente en esta zona se alojarán los documentos que no pertenezcan a procedimientos electrónicos evaluados pero que se quieran guardar en ADI, se guardaran en esta zona para disponer de ellos electrónicamente y que si en algún momento se evalúan podrían pasar a la zona de documentos administrativos o en caso contrario serán eliminados pasado el tiempo que sea estipulado. Un ejemplo son los documentos que no forman parte de procedimientos electrónicos evaluados pero que presentan por Registro electrónicamente.

Debido a la posibilidad de que un documento alojado en esta zona pueda pasar en algún momento al repositorio de documentos administrativos se aplicarán los procesos de archivo, como por ejemplo las conversiones de formato, conservación a largo plazo, etc. como en el caso de los documentos alojados en el repositorio de documentos administrativos.

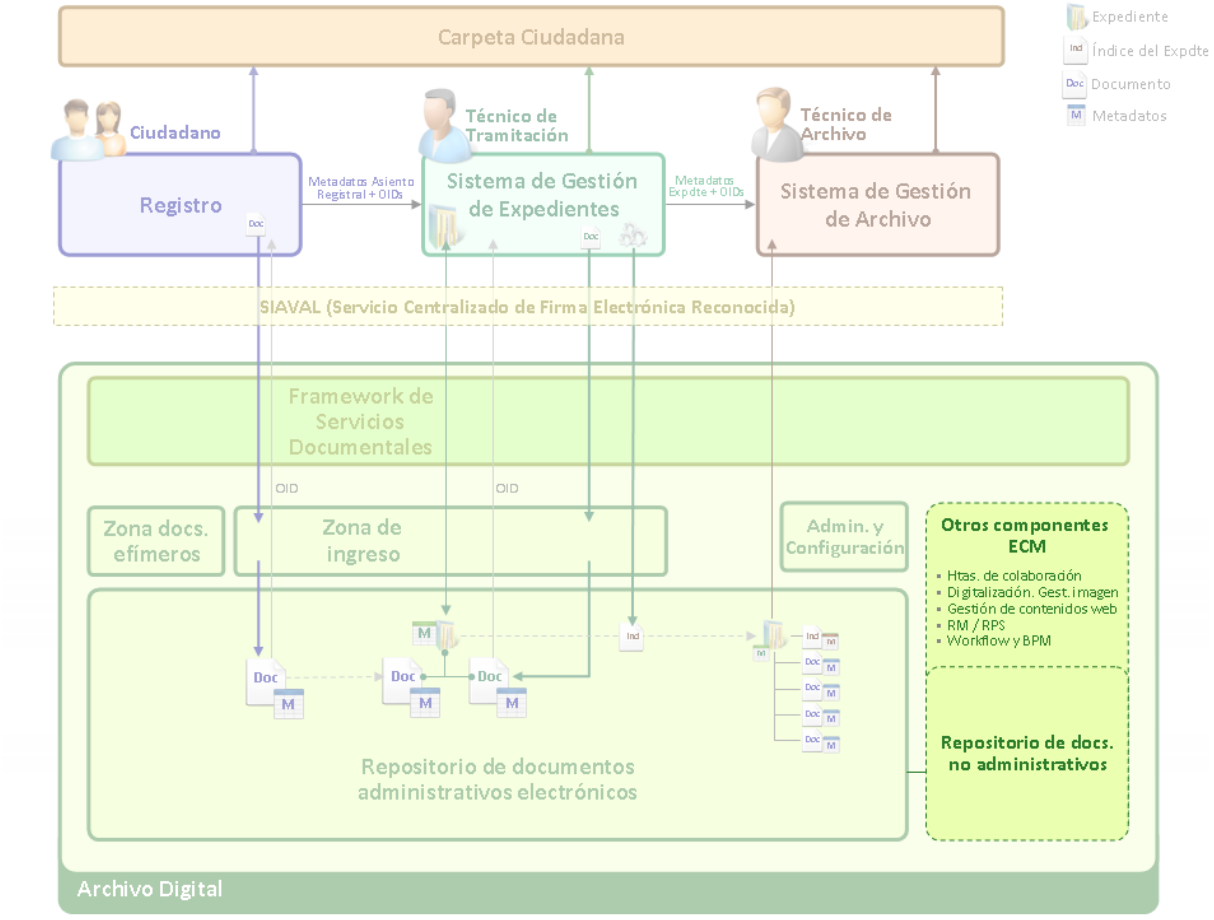


6.4.4 Repositorio de documentos no administrativos

El repositorio de documentos no administrativos permitirá la incorporación y gestión de aquellos documentos que no se generen en los procedimientos administrativos, normalmente nos referimos a copias simples que no tienen valor administrativo cuyo original se conserva.

Además también podrá ser utilizado para la gestión de aquellos documentos que forman parte de los procedimientos administrativos pero que se encuentran en fase borrador o de elaboración, y que por tanto no forman parte del repositorio de documentos administrativos electrónicos.

En este repositorio no se aplicarán los procesos de archivo, como por ejemplo las conversiones de formato, conservación a largo plazo,… [comprobación del hash]

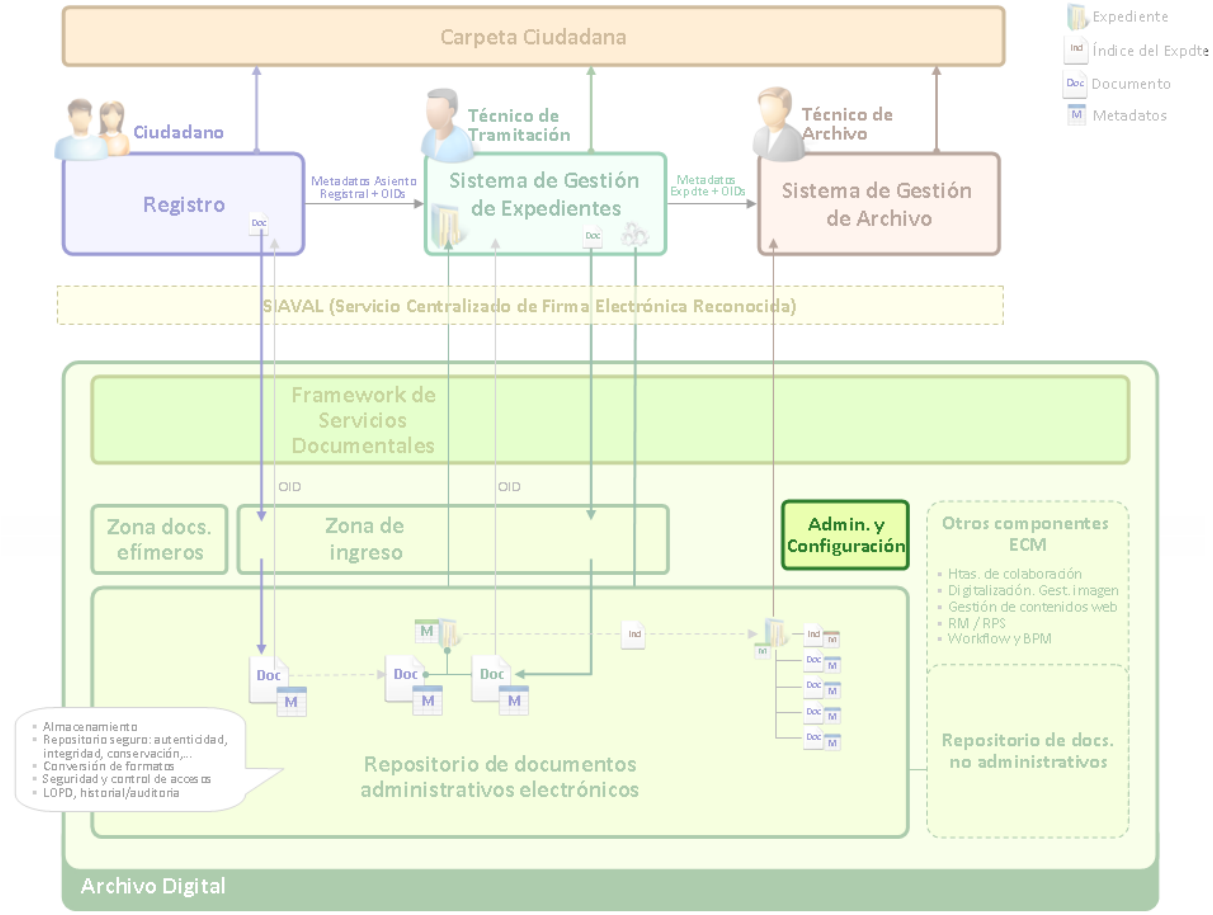


6.4.5 Administración y configuración

ADI cuenta con funcionalidades de administración y configuración.

Las principales funciones serán los siguientes:

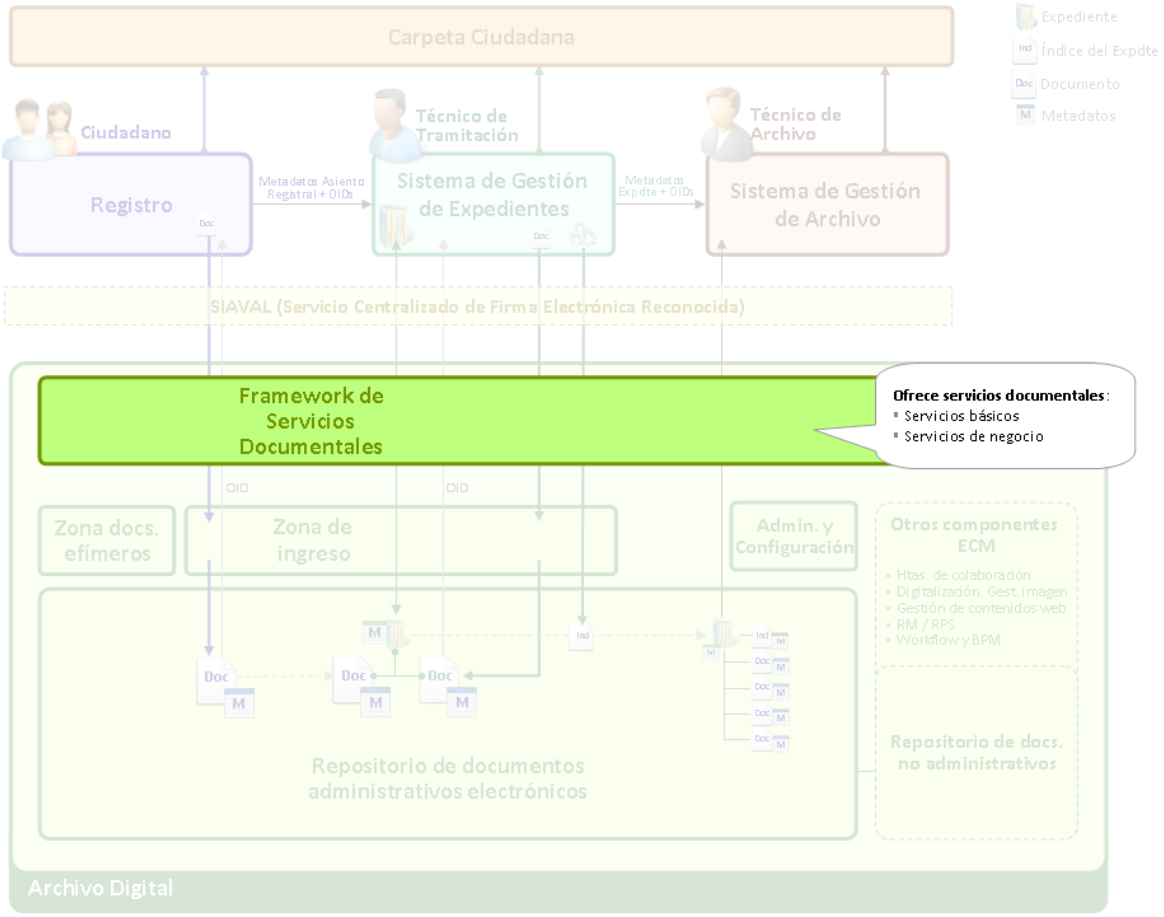
- Monitorización del sistema
- Cuadro de mando del sistema



6.4.6 Framework de servicios de gestión documental

El Framework de servicios documentales es un conjunto de servicios web de gestión documental que pueden ser invocados por los diferentes sistemas de información que se relacionen con ADI.

Todos los sistemas/aplicaciones que se relacionen con ADI deberán invocar a esta capa de servicios.



Los servicios web disponibles irán variando conforme vaya evolucionando el sistema, por lo que se mantendrá actualizada la lista de servicios web disponibles.

El API de servicios ofrecido por ADI a las distintas aplicaciones que se integrarán con él, las tecnologías usadas y las funcionalidades proporcionadas se describen en el “Manual de Integración del Archivo Electrónico”.

A continuación se enumeran los servicios ofrecidos actualmente por ADI:

Operaciones con Documentos
Alta de Documento
Consultar Documento
Borrado de Documento
Búsqueda paginada
Actualización de metadatos de Documento
Alta versión de Documento
Baja versión de documento
Consultar versión

Copiar Documentos
Recuperación de relación de copias de documento
Finalizar un Documento
Recuperación de información de firmas de un documento
Recuperación del formato de un documento

Operaciones con Expedientes
Alta de Expediente
Baja de Expediente
Asociar Documento a Expediente
Recuperación de Documentos de Expediente
Actualización de Expediente
Consultar Expediente

Operaciones con Firmas
Reemplazar Firmas

Servicios de gestión de ciclo de vida
Cerrar Expediente
Transferir Expediente

Servicios de control de formatos
Recuperación de formatos disponibles

Servicios de preservación digital
Conversión de formatos obsoletos

Servicios de exportación
Servicio de impresión documental
Servicio de generación de índice electrónico

Servicios de gestión de Procedimientos
Alta de procedimiento
Baja de procedimiento
Modificar procedimiento
Consultar procedimiento
Recuperación de procedimientos disponibles

Servicios de gestión de tipos documentales
Recuperación de tipos documentales

7 ANEXO: TÉRMINOS Y DEFINICIONES

@firma: Plataforma de validación y firma electrónica multi-PKI, que se pone a disposición de las Administraciones Públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada.

Acto administrativo: Es una manifestación de voluntad de la administración pública, expresada en el ejercicio de una potestad administrativa, con el objeto de producir efectos jurídicos para la consecución de un fin administrativo, siendo esta actuación susceptible de control por la jurisdicción contencioso-administrativa.

Actuación administrativa automatizada: Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular.

ADI o Archivo Digital: Sistema que implementa las funciones de: creación, almacenamiento, consulta, conservación, eliminación, etc. Estas funciones se exponen a través de los servicios publicados en el framework.

Archidoc: Sistema corporativo (ver Sistema de Gestión de Documentos de Archivo) encargado de la gestión de documentos en su fase inactiva. Implantado en el Archivo de la Administración.

Se utilizan dos versiones:

- Archidoc cliente-servidor (en los propios archivos).
- Archidoc web (para consulta y petición desde otras unidades).

Archivo de la Administración: Archivo Intermedio de Gobierno de Navarra que tiene entre otras funciones la identificación y valoración de series documentales y la eliminación de documentos que determine la Comisión de Evaluación Documental.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. (Esquema Nacional de Seguridad)

Un documento auténtico (ISO 15489) es aquel del que se puede probar:

- Que es lo que afirma ser
- Que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado
- Que ha sido creado o enviado en el momento en que se afirma

Autoridad de Certificación (AC): Una Autoridad de certificación, certificadora o certificante es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. La Autoridad de Certificación verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad. Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la Autoridad de Certificación utilizando su clave privada. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

Captura: Conjunto de procesos encaminados a la incorporación de un documento en el Sistema de Archivado Electrónico. Incluye registro, clasificación y adición de metadatos. (Adaptación de la definición de Moreq2).

CA (Certification Authority): Autoridad de Certificación en inglés.

CAdES: Acrónimo de CMS Advanced Electronic Signatures (Firma electrónica avanzada CMS) es un conjunto de extensiones a las recomendaciones CMS haciéndolas adecuadas para la firma electrónica avanzada. Especifica perfiles precisos de CMS para ser usados con firma electrónica reconocida con el sentido de la directiva 1999/93/EC de la Unión Europea.

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

- CAdES-BES (Basic Electronic Signature), forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada,
- CAdES-EPES (Explicit Policy based Electronic Signature), forma básica a la que se la ha añadido información sobre la política de firma.
- CAdES-T (with Timestamp), añade un campo de sellado de tiempo para proteger contra el repudio,
- CAdES-C (Complete validation data), 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),
- CAdES-X (eXtended validation data), añade sellos de tiempo a las referencias introducidas por XAdES-C para evitar que pueda verse comprometida en el futuro una cadena de certificados,
- CAdES-X-L (eXtended Long electronic signatures with time), 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,
- CAdES-A (Archiving validation data), 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.

Ciclo de vida: Distintas fases por las que atraviesa un documento desde su captura hasta su disposición final, marcada por la Comisión de Evaluación Documental, y que puede ser la eliminación o la conservación permanente.

Ciudadano: Personas física, persona jurídica o ente sin personalidad que se relacione, o sea susceptible de relacionarse, con las Administraciones Públicas.

Clasificación: Identificación y estructuración sistemáticas de las actividades de las organizaciones o de los documentos generados por éstas en categorías, de acuerdo con convenciones, métodos y normas de procedimiento, lógicamente estructurados y representados en un sistema de clasificación. (ISO 15489).

CMS (Cryptographic Message Syntax): Es el estándar del IEFT (Internet Engineering Task Force) para proteger mensajes criptográficamente. Se puede usar para firmar digitalmente cualquier tipo de dato.

Tiene como origen las especificaciones de PKCS#7 y es, a su vez, el origen de la familia de estándares CAdES.

Comisión de Evaluación Documental: Órgano asesor de la Administración con las funciones de determinar los criterios de valoración de las series documentales para la eliminación o conservación permanente y acceso a los documentos de archivo (Decreto Foral 75/2006).

Conservación: Procesos y operaciones realizados para garantizar la permanencia intelectual y técnica de documentos de archivo auténticos a lo largo del tiempo. (ISO 15489)

Copia auténtica: Documento expedido por un órgano con competencias atribuidas para ello, y con un valor probatorio pleno sobre los hechos o actos que documente, equivalente al documento original.

CSV (Código Seguro de Verificación): Es el código único que identifica a un documento electrónico en la Administración Pública española.

Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente (Ley 11/2007 de Acceso Electrónico).

Custodia electrónica: Proceso que procura guardar con cuidado y vigilancia (diccionario RAE) los documentos electrónicos.

Los objetos custodiados electrónicamente deben garantizar:

- integridad, que impida cualquier cambio sobre el original.
- su autenticidad, permitiendo contrastar su origen y ofrecer certeza sobre su autoría.
- la posibilidad de localización, facilitando las búsquedas y sin depender de relaciones externas entre la referencia y el contenido.
- el control de acceso.
- la trazabilidad de los accesos y del ciclo de vida.
- su preservación a largo plazo.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento. (Esquema Nacional de Interoperabilidad).

Digitalización certificada: Técnica que permite convertir documentos en papel a formato digital asegurando que la imagen es fiel e íntegra y que el resultado de la digitalización no puede ser modificado.

Disponibilidad: Un documento disponible es aquel que puede ser localizado, recuperado, presentado e interpretado. (ISO 15489).

Documento: Información de cualquier naturaleza archivada en un soporte y susceptible de identificación y tratamiento diferenciado.

Documento administrativo electrónico: Objeto digital administrativo que contiene la información objeto (datos) y los datos asociados a ésta (firma y metadatos). En el marco del ENI, este concepto incluye tanto los documentos electrónicos producidos por las Administraciones públicas en el ejercicio de sus competencias como los documentos electrónicos aportados por los ciudadanos en el contexto de un procedimiento dado.

- Documentos preliminares: versiones previas de un documento que se generan durante la tramitación. Son documentos que pueden tener correcciones, ampliaciones y modificaciones, hasta que su contenido queda expresado de forma definitiva.
- Documentos finales: son expresiones definitivas e inalterables de un documento administrativo electrónico.

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

Eliminación: Proceso de destrucción o borrado de documentos electrónicos de archivo de forma que no sea posible reconstrucción alguna (Moreq2).

ENI (Esquema Nacional de Interoperabilidad): Comprende el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

Se define en la Ley 11/2007 y se regula por el RD 4/2010.

ENS (Esquema Nacional de Seguridad): La finalidad del Esquema Nacional de Seguridad es crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Se define en la Ley 11/2007 y se regula por el RD 3/2010.

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

Evidencia electrónica: Son datos que, de manera digital, se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática. Tienen la función de servir como prueba física (por encontrarse dentro de un soporte) de carácter intangible (no modificables) en las investigaciones informáticas (definición del INTECO).

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

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

Expediente mixto: Un conjunto de documentos de archivo, electrónicos y tradicionales, relacionados entre sí, y conservados en parte en soporte electrónico y en parte como expediente tradicional, en papel, fuera de ADI.

Extr@: Sistema de tramitación corporativo de Gobierno de Navarra.

Evaluación documental: Valoración, sobre cada serie documental, de los criterios llamados al establecimiento de los plazos de conservación en cada una de las fases del ciclo de vida de los documentos, a la determinación de la posible eliminación total o parcial y a la accesibilidad a los mismos. (Ley 12/2007 de Archivos y Documentos).

Fiabilidad: Un documento fiable es aquel cuyo contenido puede ser considerado una representación completa y precisa de las operaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores operaciones o actividades. (ISO 15489).

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

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 (Ley 59/2003 de firma electrónica).

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. (Ley 59/2003 de firma electrónica).

Fondo: El total de documentos que una persona física o jurídica acumula con motivo de su función o actividad. Es el nivel superior de agregación archivística.

Framework de Servicios Documentales: Capa de servicios, a través de la cual acceden las aplicaciones externas a las funciones de Archivo Digital.

Identificación (documental): Estudio exhaustivo de cada serie documental destinado a proporcionar los datos necesarios para su evaluación. (Decreto Foral 75/2006. Comisión de Evaluación Documental).

Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada (Esquema Nacional de Seguridad).

Interoperabilidad: Habilidad de organizaciones y sistemas dispares y diversos para interaccionar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones.

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

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan (Esquema Nacional de Interoperabilidad).

Los metadatos pueden estar incrustados en el documento electrónico o ser gestionados en otros ficheros o bien mediante bases de datos.

Normas de conservación: Decisiones de evaluación documental que incluyen los períodos de conservación en cada fase del ciclo de vida, la accesibilidad y la disposición final para cada una de las series generadas por una institución en el desarrollo de las funciones que le son propias. (Ley 12/2007 de Archivos y Documentos).

Notificación: Acto administrativo de comunicación al ciudadano de carácter informativo o resolutivo que debe ser formalizado por una norma específica.

NTI (Norma Técnica de Interoperabilidad): Las Normas Técnicas de Interoperabilidad desarrollan una colección de aspectos más concretos que por la naturaleza de su contenido tienen difícil cabida en el real decreto que regula en ENI. Abordan cuestiones tales como las relativas al documento electrónico, a los modelos de datos, a los estándares, a la conectividad, entre otros. Las normas son:

- Catálogo de estándares (03.10.2012).
- Documento electrónico (19.07.2011).
- Digitalización de documentos (19.07.2011).
- Expediente electrónico (19.07.2011).
- Política de firma electrónica y de certificados de la Administración (19.07.2011).
- Protocolos de intermediación de datos (28.05.2012).
- Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras administraciones (28.05.2012).
- Política de gestión de documentos electrónicos (28.05.2012).
- Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas (19.07.2011).
- Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos (19.07.2011).
- Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (19.07.2011).
- Declaración de conformidad con el Esquema Nacional de Interoperabilidad (en elaboración).
- Reutilización de recursos de información (19.02.2013).

Open Data: Es una iniciativa mundial que pretende que los datos e información de las Administraciones Públicas se expongan y hagan accesibles de forma que estén disponibles para su redistribución, reutilización y aprovechamiento por parte de los ciudadanos y las empresas.

PKCS (Public-Key Cryptography Standards): Grupo de estándares de criptografía de clave pública concebidos y publicados por los laboratorios de RSA (Rivest, Shamir & Adleman).

De este grupo, concretamente PKCS#7, es el estándar usado para firmar y/o cifrar mensajes en PKI. Supuso la base del desarrollo del estándar CMS.

PKI (Public Key Infraestructure): Una Infraestructura de Clave Pública (en inglés, PKI) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

En una operación criptográfica que use PKI, intervienen conceptualmente como mínimo las siguientes partes:

- Un usuario iniciador de la operación.
- Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, Autoridad de registro y sistema de Sellado de tiempo).
- Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del

usuario iniciador de la operación (puede ser él mismo).

Plataforma de firma: Conjunto de módulos que permiten el trabajo con firma digital y custodia de documentos. Sus principales funcionalidades son:

- Generación de firmas electrónicas.
- Verificación de firmas electrónicas.
- Verificación de certificados electrónicos.
- Cifrado de documentos.
- Descifrado de documentos.
- Sellado de documentos.
- Archivado de documentos.
- Custodia electrónica.

Plataforma UCM (ECM): Plataforma ECM (Enterprise Content Manager) de Oracle, que es el núcleo de servicios documentales. Básicamente consta de:

- UCM: Sistema de almacenamiento donde reside el modelo de datos de Archivo Digital. Almacena el modelo de clasificación documental y los metadatos de los documentos electrónicos archivados, así como los catálogos y objetos necesarios para la administración del sistema de Archivo.
- Almacén de Ficheros: Sistema en el que se almacenan los ficheros con el contenido de los documentos electrónicos.

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

Procedimiento Administrativo: Secuencia ordenada de actuaciones que se siguen para la formación de la voluntad de la Administración Pública expresada en términos de actos administrativos, sobre materias de su competencia. Estos Actos Administrativos están desarrollados conforme a un ordenamiento jurídico ya establecido que puede ser conocido y fiscalizado por los ciudadanos.

Productor: Persona o institución que produce, reúne y/o conserva documentos en el desarrollo de su actividad.

Registr@: Sistema de Registro presencial del Gobierno de Navarra. Es el sistema que provee de nº de registro a todos los documentos de entrada y salida de la Administración (sean electrónicos o no).

RGE: Sistema de Registro Electrónico del Gobierno de Navarra.

Sello electrónico: Sistema de firma electrónica basado en certificado electrónico, que reúna los requisitos exigidos por la legislación de firma electrónica, que podrá ser utilizado por las Administraciones Públicas, órganos o entidades de derecho público, para la identificación y autenticación de la competencia en la actuación administrativa automatizada.

Serie documental: Conjunto de documentos producidos en el desarrollo de una misma actividad administrativa y regulado por la misma norma jurídica y de procedimiento; o documentos producidos de manera continuada como resultado de una misma actividad. (Ley 12/2007 de Archivos y Documentos).

SIAVAL: Plataforma de Firma Electrónica instalada en Gobierno de Navarra.

Sistema de gestión de documentos de archivo: Sistema de información que incorpora, gestiona y facilita el acceso a los documentos de archivo a lo largo del tiempo (ISO 15489).

Sistema de gestión documental: Marco en el que se definen, implantan y evalúan los principios metodológicos, las técnicas y los instrumentos que sirven de fundamento básico al desarrollo de políticas y normas, destinadas a regir el tratamiento de los documentos a lo largo de las etapas de su ciclo de vida, con diferentes regulaciones para su organización, conservación, tratamiento y accesibilidad en cada etapa (Ley 12/2007 de Archivos y Documentos).

Sistema de Registro: Aplicaciones encargadas de canalizar la entrada y salida de documentos oficiales.

Sistema de Tramitación: Sistema de información encargado de la tramitación de procedimientos administrativos.

Timestamp: Sello de tiempo.

Trámite (o actividad administrativa): Conjunto de tareas ejecutadas, según normativa vigente, por un recurso humano y/o tecnológico que implica una entrada/salida de datos o documentación.

Transferencia: Cambio de la custodia, la propiedad y/o la responsabilidad de los documentos de archivo (ISO 15489).

Trazabilidad: Creación, incorporación y conservación de información sobre el movimiento y el uso de documentos de archivo (ISO 15489).

Valor de los documentos: Valor administrativo, legal, fiscal, contable (valores primarios del documento) y valor histórico, científico o cultural (valores secundarios).

W3C: Acrónimo de World Wide Web Consortium, es un consorcio internacional que promueve especificaciones para la World Wide Web.

XAdES: Acrónimo 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. Especifica perfiles precisos de XML-DSig para ser usados con firma electrónica reconocida con el sentido de la directiva 1999/93/EC de la Unión Europea.

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

- XAdES-BES (Basic Electronic Signature), forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada,
- XAdES-EPES (Explicit Policy based Electronic Signature), forma básica a la que se la ha añadido información sobre la política de firma.
- XAdES-T (with Timestamp), añade un campo de sellado de tiempo para proteger contra el repudio,
- XAdES-C (Complete validation data), 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 validation data), 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 electronic signatures with time), 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 (Archiving validation data), 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.

XML: Acrónimo de eXtensible Markup Language (lenguaje de marcas extensible), es un metalenguaje extensible de etiquetas desarrollado por el W3C. No es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades, de ahí que se le denomine metalenguaje.

XMLDSig (Firma XML, DSig XML o XML-Sig): Es una recomendación del W3C que define una sintaxis XML para la firma electrónica. Funcionalmente, tiene mucho en común con PKCS#7, pero es más extensible y está orientada hacia la firma de documentos XML.

Las firmas XML se pueden utilizar para firmar datos o recursos de cualquier tipo, normalmente documentos XML, pero cualquier cosa que sea accesible a través de una URL puede firmarse. Una firma XML que se utiliza para firmar un recurso fuera del documento XML que la contiene se llama una firma separada (detached). Si se utiliza para firmar una parte del documento que la contiene, se llama una firma envuelta (enveloped). Si contiene los datos firmados dentro de sí mismo se llama una firma envolvente (enveloping).