

JOSE MARIA ASIRON SAEZ -
29/09/2016 12:08:55

Original firmado electrónicamente



Ayuntamiento de
Pamplona
Iruñeko Udala

Plan Director del Documento Electrónico del Ayuntamiento de Pamplona

Pamplona, enero de 2016

ÍNDICE

1. VISIÓN Y OBJETIVOS	6
2. MARCO NORMATIVO Y ESTÁNDARES INTERNACIONALES	8
2.1 Normativa aplicable	9
2.2 Estándares internacionales y otras convenciones	18
3. EL SISTEMA DE GESTIÓN DOCUMENTAL Y EL CICLO DE VIDA DE LOS DOCUMENTOS	27
3.1 Introducción	27
3.2 Alcance del modelo documental	28
3.3 Ciclo de vida de los documentos	28
3.4 Modelo propuesto	30
3.5 Los procesos de gestión de documentos del sistema	33
3.6 Arquitectura tecnológica del Ayuntamiento de Pamplona	44
3.7 Aplicación del modelo documental a casos concretos	53
4. CASOS DE USO	54
4.1 Casos de uso sobre tipologías de procedimiento	54
4.2 Ejemplo de arquitectura tecnológica de gestión documental	63
4.3 Ejemplo de un proceso de digitalización masivo: interno y externo.	63
4.4 Ejemplo de un sistema de preservación de documentos.	65
4.5 Ejemplo de un sistema de preservación de la firma de documentos.	66
5. MODELO ORGANIZATIVO	67
5.1 Necesidad de un modelo organizativo	67
5.2 Gestión del cambio	68
5.3 Metodología de simplificación y reingeniería de procesos	70
5.4 Metodología de aplicación del modelo a un expediente concreto	73

5.5	Responsabilidades en la aplicación de la Política Documental	74
6.	MODELO TECNOLÓGICO DEL DOCUMENTO Y EXPEDIENTE ELECTRÓNICO	77
6.1	Representación del expediente y documento electrónico	77
6.2	El ciclo de vida de los documentos electrónicos en los entornos tecnológicos de gestión documental del Ayuntamiento	78
6.3	Herramientas archivísticas de base y metodología para su construcción	92
6.4	Ficha de aplicación del modelo tecnológico del documento y expediente electrónico	105
7.	MODELO DE DIGITALIZACIÓN SEGURA Y COPIA AUTÉNTICA	109
7.1	Fundamento jurídico	109
7.2	Escenarios de digitalización	110
7.3	Procedimiento de digitalización Segura	117
7.4	Requisitos del proceso de digitalización	119
7.5	Ejecución de la Digitalización	122
7.6	Formatos de digitalización	126
7.7	Metadatos de digitalización segura	127
7.8	Habilitación de la digitalización	128
8.	MODELO DE IMPRESIÓN SEGURA	131
8.1	Fundamento jurídico	131
8.2	Uso de la impresión segura en el Ayuntamiento de Pamplona	132
8.3	Procedimiento de generación	133
8.4	Procedimiento de validación	135
8.5	Custodia de los elementos de verificación	136
8.6	Habilitación jurídica	137
9.	MODELO DE PRESERVACIÓN	137
9.1	Definición de la estrategia de preservación de los documentos y expedientes electrónicos	138
9.2	Selección de formato de conservación	139

9.3	Requerimientos de los elementos a transferir.	141
9.4	Identificación de las circunstancias en que las actividades de migración se llevarán a cabo y de los métodos y los fundamentos para realizarlas.	141
9.5	Soluciones tecnológicas	143
9.6	Tipo de integración de la solución tecnológica con la herramienta de gestión documental y archivo	174
9.7	Responsabilidades de los actores intervinientes en la preservación de los Documentos y Expedientes Electrónicos.	177
10.	MODELO DE SEGURIDAD DEL DOCUMENTO Y EXPEDIENTE ELECTRÓNICO	181
10.1	Conceptos del modelo de seguridad	183
10.2	Autenticación de los usuarios	185
10.3	Recuperación de la información y la documentación	186
10.4	Monitorización de la información y la documentación	188
10.5	Acceso a la plataforma tecnológica de gestión de documentos y expedientes electrónicos	190
10.6	Aplicación del modelo de seguridad documental	199
11.	POLÍTICA DE USO DEL CERTIFICADO DIGITAL Y LA FIRMA ELECTRÓNICA	204
11.1	Introducción.	204
11.2	Objeto	204
11.3	Datos identificativos de la política.	205
11.4	Conceptos	205
11.5	Normativa aplicable y estándares internacionales.	206
11.6	Uso de certificados digitales	210
11.7	Ciclo de vida de la firma electrónica: creación, verificación y conservación.	211
11.8	Sello de tiempo	212
11.9	Clases, tipos y niveles de firma.	213
11.10	Mantenimiento de las firmas	220
11.11	Metadatos de firma.	222

11.12	Casos de uso de la firma electrónica.	223
12.	GLOSARIO DE TERMINOLOGÍA	229
13.	ANEXO I. CUESTIONARIOS PARA EL ANÁLISIS DE PROCEDIMIENTOS	232
	Cuestionario para el análisis del flujo	232
	Cuestionario para el análisis de los roles	233
	Cuestionario para el análisis de los documentos	234
14.	ANEXO II: PROYECTO DE DIGITALIZACIÓN	235
	1. Actividades previas al proceso	235
	2. Implementación técnica	237
	3. Actividades posteriores al proceso	237
15.	ANEXO III: REQUERIMIENTOS TÉCNICOS MÍNIMOS QUE DEBE TENER UN HARDWARE Y SOFTWARE PARA UNA DIGITALIZACIÓN SEGURA DE DOCUMENTOS ELECTRÓNICOS.	238
	1. Requisitos de los dispositivos de captura de imagen	238
	2. Requisitos del software de digitalización	241
	3. Requisitos del sistema de firma electrónica	242
	4. Requisitos de la imagen electrónica	242
2.	ANEXO IV: REQUERIMIENTOS PARA LA DIGITALIZACIÓN EXTERNALIZADA	246
	1. Modelos de cláusulas para regir la digitalización externalizada	247

1. Visión y objetivos

En los últimos años, el Ayuntamiento de Pamplona (en adelante, el Ayuntamiento) ha estado trabajando para modernizar sus procesos de gestión y adecuarse a las novedades que la tecnología y los cambios legislativos están introduciendo en la gobernanza de las administraciones públicas.

En el marco del impulso dado por la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos y, a partir del 2 de octubre de 2016, por la ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, el Ayuntamiento ha regulado en un único cuerpo normativo los aspectos relacionados con la Administración electrónica, concretamente en la *Ordenanza reguladora de la Administración electrónica del Ayuntamiento de Pamplona* aprobada según el Acuerdo del Pleno de fecha 17 de septiembre de 2010 y publicada en el Boletín Oficial de Navarra número 153, de 17 de diciembre de 2010.

En este marco, el Ayuntamiento ha decidido que no sólo hay que dar cumplimiento a los requerimientos de la ley de relación telemática con la ciudadanía, sino aprovechar la oportunidad para extraer los máximos beneficios de la utilización de las tecnologías de la información para simplificar sus procesos de gestión, incrementar la eficiencia y reducir los costes, directos e indirectos.

El Ayuntamiento ha optado, por tanto, por establecer un modelo de gestión basado en el uso de documentos electrónicos o gobernanza electrónica, con el objetivo de que la modernización de su infraestructura tecnológica permitirá garantizar:

- **Eficacia en la gestión** - La incorporación de herramientas de tramitación y gestión de expedientes agilizará el funcionamiento de la organización y dará mayores garantías de la consecución de los objetivos.
- **Eficiencia en el aprovechamiento de los recursos** - Reduciendo el tiempo que se invierte en la gestión de documentos en papel, ahorrando en espacio destinado a su archivo, reduciendo el número de desplazamientos e incluso el propio consumo de materiales.
- **Seguridad de la información** - La definición de sistemas de preservación documental permite aplicar mecanismos automatizados para controlar el acceso a la documentación y garantizar la conservación a largo plazo del conocimiento de la organización.
- **Transparencia** - El hecho de que la documentación esté disponible en un soporte fácilmente compartible da adecuada respuesta también a la voluntad de someter a escrutinio público la labor del Ayuntamiento.
- **Cumplimiento normativo** - No menos importante es el objetivo de dar respuesta a las obligaciones impuestas por diferentes leyes que han ido apareciendo últimamente, muy especialmente las Leyes 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos y a partir del 2 de octubre de 2016, las leyes

39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de Régimen Jurídico del Sector Público, pero también las leyes que establecen la necesidad de practicar una mejora y simplificación de procedimientos y una reducción de cargas administrativas como es la Directiva Europea de Servicios 2006/123/CE.

Este modelo de gestión basado en el uso del documento electrónico, se define en el presente Plan Director del Documento Electrónico el cual pretende el establecimiento de un conjunto de directrices, herramientas, procedimientos, prácticas y normas con la finalidad de garantizar una gestión eficiente de los documentos y los expedientes electrónicos a lo largo de todo su ciclo de vida, es decir, desde su generación, captura o incorporación al sistema hasta su disposición final (eliminación o conservación permanente). Este Plan tiene como principal finalidad asegurar que los documentos que se gestionan son auténticos, fiables, íntegros y que sirven al objetivo de apoyar las funciones y actividades del Ayuntamiento por el tiempo que se determine.

En definitiva, la vocación del Plan Director del Documento Electrónico es la de regular todos los aspectos relacionados con la gestión de documentos electrónicos dentro del Ayuntamiento. En este sentido, el Plan Director del Documento Electrónico debe convertirse en un documento vivo, que el Ayuntamiento adecuará a los cambios tecnológicos y normativos que se vayan sucediendo en el tiempo.

Para dotar al Plan Director del Documento Electrónico de reconocimiento formal dentro de las actividades del Ayuntamiento, éste se establece como una de las disposiciones de desarrollo de la Ordenanza de administración electrónica tal y como se prevé en la Disposición Adicional Primera y se aprobará por el Órgano de Gobierno Municipal competente en esta materia. De este modo la alta dirección del Ayuntamiento se convierte en el máximo impulsor del propio Plan garantizando su sostenibilidad mediante la asignación de los recursos humanos y económicos adecuados.

Por último, cabe mencionar que el ámbito de aplicación del Plan es el Ayuntamiento de Pamplona y sus entidades vinculadas afectando a la totalidad de su personal, tanto de carácter funcional como contratado, sea en grado de dependencia directa del Ayuntamiento o a través de empresas externas mediante convenio o cualquier otra modalidad contractual. Por lo tanto, este Plan debe aplicarse a todos los documentos electrónicos, creados y recibidos por el Ayuntamiento y entidades vinculadas en la medida que son testimonio y evidencia de sus actividades, con independencia de su fecha de creación.

2. Marco normativo y estándares internacionales

La reciente revolución en el uso del documento electrónico resulta de la aparición de cambios normativos, que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como en la Unión Europea o internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos garantizando su validez jurídica.

Algunas de las decisiones que se reflejarán en el Plan Director del Documento Electrónico estarán condicionadas o basadas en esta normativa o estos estándares. Aunque este Plan debe ser suficientemente detallado como para ofrecer soluciones concretas a la gestión diaria de la actividad del Ayuntamiento, tanto a efectos de interpretación como de la futura extensión y desarrollo del Plan, se debe tener identificado este marco normativo.

Lo que se presenta a continuación es la identificación de:

- Normas, clasificadas en función de su rango y ámbito territorial, que regulan diferentes aspectos asociados a la gestión documental.
- Estándares internacionales, clasificados en función de la materia, que han servido para informar a las normas anteriores o que se aplican de manera generalizada en los procesos de gestión documental.

2.1 Normativa aplicable

2.1.1 Normativa del Ayuntamiento de Pamplona

Ordenanza de Administración Electrónica	Ordenanza reguladora de la Administración electrónica del Ayuntamiento de Pamplona aprobada según el Acuerdo del Pleno de fecha 17 de septiembre de 2010 y publicada en el Boletín Oficial de Navarra número 153, de 17 de diciembre de 2010
<p>La ordenanza regula la utilización de los medios electrónicos en el ámbito del Ayuntamiento de Pamplona y formaliza un modelo de gestión y de relación que el Ayuntamiento ya venía usando desde hace años. Sus objetivos son:</p> <ol style="list-style-type: none"> Facilitar el acceso electrónico de los ciudadanos a la información y a los servicios del Ayuntamiento, facilitando el cumplimiento de los derechos y deberes en este ámbito. Generar confianza en la ciudadanía y garantizar la protección de los datos de carácter personal y la intimidad y privacidad de las personas. Promover las medidas de transparencia y la proximidad con los ciudadanos. Mejorar el funcionamiento interno del Ayuntamiento, contribuyendo a la simplificación de los procedimientos internos mediante las TIC. <p>Para la consecución de estos objetivos, esta Ordenanza regula fundamentalmente los siguientes aspectos:</p> <ul style="list-style-type: none"> Establece los principios generales que rigen la Administración Electrónica en el Ayuntamiento de Pamplona (Art. 4). Reconoce derechos y deberes de los ciudadanos en materia de administración electrónica (Art. 5 y 6). Establece la Sede Electrónica, la Carpeta Ciudadana y el Tablón de Edictos Electrónico (Art. 7 y 8) Se regulan los medios de identificación con los que los ciudadanos se pueden relacionar con el Ayuntamiento (Art. 9) Se regulan asimismo los medios que utilizará la Administración municipal para identificarse y firmar documentos electrónicos (Art. 10 a 15). Regula la transparencia y publicidad de la información municipal (Art. 16 a 18). Crea y regula el registro electrónico municipal (Art. 19 a 28). Regula el uso del documento y expediente electrónicos, así como los procesos para generar copias electrónicas auténticas (Art. 29 a 32). Regula el procedimiento administrativo electrónico, incluidos los mecanismos de interacción con el ciudadano (comunicaciones y notificaciones electrónicas), en los artículos 33 a 47. Describe el proceso a través del cual se pondrán en funcionamiento nuevos procedimientos en soporte electrónico (Art. 50 a 53). Regula el uso de la factura electrónica en el Ayuntamiento (Art 48) 	

2.1.2 Normativa autonómica

Ley Foral 11/2007	De 4 de abril, de Implantación de la Administración Electrónica
<p>Es previa a la Ley Estatal (4 de Abril), pero define fundamentalmente los mismos conceptos que ésta:</p> <ul style="list-style-type: none"> • Identifica los derechos del ciudadano en este ámbito. • Define instituciones como el Registro Electrónico. • Describe el funcionamiento de los documentos electrónicos administrativos y notificaciones electrónicas. • En su capítulo V entra en detalle sobre el uso de la Firma Electrónica en el Sector Público 	

Ley Foral 12/2007	De 4 de abril, de Archivos y Documentos
<p>Define el Sistema Archivístico de Navarra y las competencias de la Comisión de Evaluación Documental. Describe el ciclo de vida de los archivos y las responsabilidades y funciones de los diferentes actores.</p> <p>De acuerdo con lo que establece en su artículo 28 y siguientes, los archivos municipales están sujetos a esta ley y deben integrarse en el sistema de Archivos de Navarra.</p> <p>En su artículo 29 establece la obligación, para los municipios de mayor tamaño, de disponer de un sistema archivístico propio y de un archivo municipal que cumpla una serie de funciones que se detallan y disponga de los medios técnicos apropiados.</p>	

Ley Foral 14/2005	De 22 de noviembre, del Patrimonio Cultural de Navarra
<p>Esta Ley desarrolla las competencias de la Comunidad Foral en materia de cultura, y contempla específicamente el acervo documental dentro del patrimonio cultural.</p> <p>En su artículo 12 crea la Comisión de Evaluación Documental, que es un órgano con competencias para determinar los criterios de eliminación y conservación de los documentos de archivo.</p>	

Decreto Foral 75/2006	De 30 de octubre, regulador de la Comisión de Evaluación Documental
<p>Crea formalmente este órgano asesor y regula sus competencias, composición y funcionamiento.</p>	

2.1.3 Legislación estatal

En materia de archivos y gestión documental, en el ámbito de la administración local, la competencia recae en la Comunidad Foral, por lo que en este ámbito la normativa del estado sólo se aplica a efectos interpretativos o de manera subsidiaria. En lo que hace

referencia a procedimiento administrativo y administración electrónica, la normativa estatal es de directa aplicación (Leyes 11/2007, 39/2015, 40/2015, ENI, ENS, etc.).

Ley 16/1985, 25 de junio	Patrimonio Histórico Español
<ul style="list-style-type: none"> • Definición amplia del concepto patrimonio histórico • Delimita su ámbito de aplicación al patrimonio documental de carácter histórico • Concepto de documento • Falta de concreción en cuanto a los archivos y documentos administrativos 	

Real Decreto 1708/2011, de 18 de noviembre	Establece el Sistema Español de Archivos
<ul style="list-style-type: none"> • Establece el Sistema Español de Archivos • Creación del Consejo de Cooperación Archivística • Formula directrices para coordinar los criterios archivísticos • Creación de la Comisión de Archivos de la Administración General del Estado • Establece criterios básicos para el ejercicio del derecho de acceso a los archivos 	

Real Decreto 1164/2002, de 8 de noviembre	Conservación del Patrimonio Documental con valor histórico, control de la eliminación de documentos y conservación en soporte distinto al original
<ul style="list-style-type: none"> • Caracteriza el régimen de eliminación • Define documentos con valor probatorio • Condiciones para la sustitución de apoyos • Define dictámenes de la Comisión Superior Calificadora de Documentos Administrativos 	

Real Decreto 1401/2007, de 29 de octubre	Regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos.
<ul style="list-style-type: none"> • Señala objeto y finalidad de la CSCD • Caracteriza las transferencias y la accesibilidad • Define procedimiento propuestas de eliminación • Señala la composición de la CSCD 	

Ley 39/2015, 1 de octubre	Procedimiento Administrativo Común de las Administraciones Públicas
<p>Esta ley regula de manera completa y sistemática las relaciones entre Administraciones y administrados, así como de las administraciones entre ellas. Deroga por absorción tanto la Ley 30/1992 como la 11/2007. Establece, entre otros:</p> <ul style="list-style-type: none"> • Con carácter general, uso generalizado y obligatorio de medios electrónicos en las fases del procedimiento administrativo, y uso del documento electrónico como principal herramienta de gestión administrativa. • Obligación de cada Administración Pública de contar con un registre electrónico de apoderamientos. Las administraciones territoriales se pueden adherir al del Estado. • Obligación de cada Administración Pública de tener un registro electrónico general o adherirse al de la Admin. General del Estado. • Obligación de cada Administración Pública de mantener un archivo electrónico único de los documentos que correspondan a procedimientos finalizados. Obligación de guardar los expedientes en un formato que asegure la autenticidad, integridad y conservación del documento. • Obligación de la Administración Pública de no requerir documentos ya aportados por los interesados, elaborados por la Admin. Pública o documentos originales. 	

- Obligación de las Administraciones Públicas de contar con un registro u otro sistema equivalente que permita dejar constancia de los funcionarios habilitados por realizar copias auténticas.
- Introducción del cómputo de plazos por horas y declaración de los sábados como inhábiles.
- Preferencia de las notificaciones electrónicas en Sede electrónica o en dirección electrónica habilitada única
- Todas las administraciones divulgarán un Plan Anual Normativo donde se recogerán todas las propuestas de rango de ley o de reglamento que tengan que ser elevadas para su aprobación el año siguiente.
- Obligación de evaluar periódicamente la aplicación de las normas en vigor. Comprobar logro de objetivos perseguidos y ver si el coste y cargas derivadas de estos estaban justificados y valorados correctamente.

Ley 40/2015, 1 de octubre	Régimen Jurídico del Sector Público
<p>Esta ley regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora así como la organización y funcionamiento de la Administración General del Estado y su sector público institucional. Deroga las Leyes 6/1997 y la 28/2006. Establece, entre otros:</p> <ul style="list-style-type: none"> • Obliga al cumplimiento del Esquema Nacional de Interoperabilidad y del Esquema Nacional de Seguridad. • Posibilidad de realizar videoactas de las sesiones de los órganos colegiados. • Se debe garantizar la comunicación segura en la Sede electrónica • Posibilidad que las Administraciones se puedan identificar a través de sello electrónico. • Las Administraciones Públicas deberán escoger entre el sello electrónico y el código seguro de verificación vinculado al órgano o institución como sistema de firma electrónica. • Posibilidad de implementar actuaciones administrativas automatizadas para ejecutar procedimientos administrativos. • El empleado Público deberá firmar electrónicamente con la signatura propia o la del titular del órgano cuando realice procedimientos administrativos por medios electrónicos. • Se deben suscribir convenios para poder intercambiar electrónicamente datos e información entre diferentes administraciones. • Regulación de cómo se debe gestionar la documentación incluida en el Archivo electrónico. • Obligación de facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder. • Obligación de poner a disposición de otras Administraciones para su reutilización de las aplicaciones informáticas propias de las cuales la Administración Pública sea la titular. 	

Ley 11/2007, 22 de junio	Acceso electrónico de los ciudadanos a los servicios públicos
<p>(Derogada a partir del 2 de octubre de 2016 por absorción en la Ley 39/2015, del Procedimiento Administrativo Común)</p> <p>Elementos tratados en esta ley:</p> <ul style="list-style-type: none"> • Derecho del ciudadano a operar por medios electrónicos. • Usos de la firma electrónica. • Uso de documentos digitales para la administración pública. • Conservación de documentos digitales y posibilidad de generar copias auténticas. • Obligación por parte de las administraciones públicas de ofrecer interoperabilidad. • Definición de la sede electrónica. • Reutilización de sistemas y aplicaciones de propiedad de la Administración. 	

Real Decreto 1720/2007, 6 de noviembre	Desarrollo parcial de la Ley 11/2007
<p>(Derogado tácitamente por la Ley 39/2015, del Procedimiento Administrativo Común)</p> <p>Concreta el desarrollo parcial de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Esta norma es de aplicación específicamente a la Administración General del Estado, pero es interesante mantenerla como referente por el detallado desarrollo que hace de las instituciones de la Ley.</p> <ul style="list-style-type: none"> • Procura la más plena realización de los derechos reconocidos en la Ley 11/2007, facilitándoles en la medida que lo permita el estado de la técnica, y la garantía de que no resulten afectados otros bienes constitucionalmente protegidos, como pueden ser la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros. • Establece un marco lo más flexible posible en la implantación de los medios de comunicación, cuidando los niveles de seguridad y protección de derechos e intereses previstos tanto en la propia ley, como en la legislación administrativa general. • El Esquema Nacional de Interoperabilidad será el encargado de establecer los criterios comunes de gestión de la información que permitan compartir soluciones e información. • El Esquema Nacional de Seguridad, establecerá los criterios y niveles de seguridad necesarios para los procesos de tratamiento de la información que prevé el propio decreto. • Características del documento electrónico, concretamente adición de metadatos. 	

Real Decreto 3/2010, 08 de enero	Esquema Nacional de Seguridad
<p>Elementos tratados en este decreto:</p> <ul style="list-style-type: none"> • Principios básicos: seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada. • Requisitos mínimos de seguridad. • Condiciones y requisitos técnicos de las comunicaciones electrónicas. • Firma electrónica. • Auditoría de seguridad. • Respuesta a incidentes de seguridad. • Categorización de los sistemas de información, según la seguridad. • Medidas de seguridad. • Glosario. <p>Se tienen en cuenta también las Guías de Seguridad que desarrollan detalladamente la aplicación de este Decreto.</p>	

Real Decreto 4/2010, 08 de enero	Esquema Nacional de Interoperabilidad
<p>Elementos tratados en este decreto:</p> <ul style="list-style-type: none"> • Principios básicos: interoperabilidad como cualidad integral, carácter multidimensional de la interoperabilidad y enfoque de soluciones multilaterales. • La interoperabilidad desde diferentes puntos de vista: organizativo, semántico y técnico. • Infraestructuras y servicios comunes. • Reutilización y transferencia de tecnología. • Firma electrónica y certificados. • Respuesta a incidentes de seguridad. • Recuperación y conservación del documento electrónico. • Normas de conformidad y actualización permanente. • Glosario. 	

Se tienen en cuenta también las Normas Técnicas de Interoperabilidad que desarrollan detalladamente la aplicación de este Decreto.

Ley 59/2003, 19 de diciembre	Firma electrónica
Elementos tratados en esta ley: <ul style="list-style-type: none"> Definición de firma electrónica y como firmar documentos electrónicamente. Uso de la firma electrónica en el ámbito de las administraciones públicas. Regulación del marco de prestación de servicios de certificación. Definición certificado digital reconocido, necesario para la firma electrónica reconocida. Regulación del ciclo de vida de los certificados digitales: extinción, revocación, suspensión... Responsabilidades de los prestadores de servicios de certificación. Requerimientos y características de los dispositivos utilizados para la firma electrónica. Habilita la facturación electrónica. Régimen sancionador. Fe pública y uso de la firma electrónica. 	
Ley 30/2007, 30 de octubre	Contratos del Sector Público
Elementos tratados en esta ley: <ul style="list-style-type: none"> Definición de los diversos tipos de contratos. Racionalidad y consistencia de la contratación del sector público. Contenido mínimo de los contratos. Especificaciones respecto al formato y a las partes que constituyen el contrato. Régimen especial de revisión y medios alternativos para la resolución de conflictos. Certificaciones de Registros Oficiales de Licitadores y Empresas Homologadas. Órganos de contratación y de asistencia. Uso de medios electrónicos, informáticos y telemáticos en los procedimientos regulados por la ley. 	
Ley 19/2013, de 9 de diciembre	Transparencia, acceso a la información pública y buen gobierno
<ul style="list-style-type: none"> Establece obligaciones de publicidad para todas las administraciones públicas, en el sentido de publicar en un formato accesible y reutilizable determinadas informaciones relativas a la gestión pública. Establece un procedimiento para acceder, con carácter general, a cualquier documento o expediente en poder de la administración pública. 	
Ley 15/2014, de 16 de septiembre	Racionalización del sector público y otras medidas de reforma administrativa
<ul style="list-style-type: none"> Modifica los requisitos en materia de admisibilidad de certificados electrónicos, en el sentido de que las administraciones están obligadas a reconocer todos los certificados admitidos por el Ministerio de Administraciones Públicas 	
Ley 37/2007, 16 de noviembre	Reutilización de la información del sector público
Elementos tratados en esta ley: <ul style="list-style-type: none"> Definición de los documentos que se pueden reutilizar y los que no. Uso de los medios electrónicos en la reutilización. Formatos e idiomas. 	

- Contraprestaciones económicas.
- Condiciones de reutilización.
- Licencias.
- Procedimiento y régimen sancionador.

Ley 56/2007, 28 de diciembre	Medidas de Impulso de la Sociedad de la Información
<p>Elementos tratados en esta ley:</p> <ul style="list-style-type: none"> • Modificaciones legislativas para el impulso de la sociedad de la información y de las comunicaciones electrónicas. • Medidas de impulso de la factura electrónica y del uso de medios electrónicos en otras fases de los procesos de contratación empresarial. • Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario. • Definición de las obligaciones de información sobre seguridad. 	

Ley 30/1992, 26 de noviembre	Régimen jurídico de las administraciones públicas y del procedimiento administrativo
<p>Se encarga de regular el régimen jurídico de las administraciones públicas y del procedimiento administrativo común</p> <p>Elementos tratados en esta ley:</p> <ul style="list-style-type: none"> • Principios de las relaciones entre las administraciones públicas. • Conferencias sectoriales y otros órganos de cooperación. • Convenios de colaboración. • Planes y programas conjuntos. • Efectos de los convenios. • Relaciones con la administración local. • Comunicaciones con la Comunidad Europea. • Órganos de las administraciones públicas. • La actividad de las administraciones públicas. • Normas y derechos generales. • Términos y plazos. • Iniciación, ordenación, instrucción y finalización de los procedimientos. • Resolución. • Revisión de los actos en vía administrativa. 	

Ley 15/1999, 13 de diciembre	Ley Orgánica de Protección de Datos de Carácter Personal
<p>Elementos tratados en esta ley:</p> <ul style="list-style-type: none"> • Regula la protección y el uso de la información personal de los documentos. • Definición de las personas respecto a sus datos. • Definición de las características de los ficheros de titularidad pública y privada. • Establece los movimientos internacionales de datos. • Régimen de infracciones y sanciones. 	

Real Decreto 1671/2009, 21 de diciembre	Reglamento de desarrollo de la Ley Orgánica 15/1999
<p>Concreta el desarrollo de la LOPD, incluyendo cómo se han de ejecutar los procedimientos establecidos por la Ley Orgánica de Protección de Datos de Carácter Personal.</p> <ul style="list-style-type: none"> • Consentimiento para el tratamiento de los datos. 	

- Formas para obtener el consentimiento y proceso para revocarlo.
- Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.
- Regula la conservación de los datos por parte del encargado del tratamiento.
- Establece las pautas a seguir para el control de accesos, registro de incidencias, auditorías, ...
- Condiciones a establecer en los procedimientos de copias de seguridad de los datos.
- Características y procedimientos a seguir, para hacer copias de los datos.
- Procedimiento sancionador y de declaración de las infracciones.
- Desarrolla todo lo relacionado con la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones y documentos electrónicos y copias.

Real Decreto 772/1999, 7 de mayo	Solicitudes, escritos y comunicaciones ante la Administración del Estado. Expedición de copias de documentos y devolución de originales. Oficinas de Registro
---	--

Elementos tratados en este real decreto:

- Establece los medios de presentación: soporte papel, informáticos, electrónicos o telemáticos.
- Definición del procedimiento de entrega de recibos de presentación de documentos.
- Expedición de copias de documentos, definiendo el procedimiento a seguir.
- Definición del procedimiento de compulsas y de la obtención de copias auténticas de documentos públicos administrativos.
- Comunicaciones y documentos en lenguas cooficiales.
- Definición de las oficinas de registro y sus funciones, también por los registros telemáticos.

Real Decreto 209/2003, 21 de febrero	Regula los registros y las notificaciones telemáticas así como la utilización de los medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
---	---

Elementos tratados en este real decreto:

- Posibilita la sustitución de certificados administrativos con soporte electrónico.
- Identifica los contenidos básicos de un certificado administrativo en soporte electrónico así como su emisión.
- Regula el intercambio de datos como sustituto de los certificados administrativos.
- Regula cómo crear y cómo deben funcionar los registros telemáticos.

Orden CUL/1014/2007, 30 de marzo	Constituye la Comisión Española sobre la digitalización y la accesibilidad en línea del material cultural y la conservación digital.
---	---

Elementos tratados en esta orden:

- Establece la creación dentro del Ministerio de Cultura de la Comisión.
- Establece las funciones, la composición y el funcionamiento de la Comisión.

2.1.4 Normativa supranacional

Directiva 1999/93/EC, 13 de diciembre	Marco comunitario para la firma electrónica
--	--

El objetivo es facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. Crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior.

Elementos tratados en este decreto:

- Definición del mercado interior, formado por los 25 estados miembros de la Unión Europea.
- Efectos jurídicos de la firma electrónica, establece unos requisitos jurídicos que todos los miembros deberán procurar cumplir, por la firma avanzada basada en un certificado digital reconocido.
- Protección de datos, los miembros deberán velar por cumplir con lo establecido en la directiva 95/46/EC del Parlamento Europeo y del Consejo, 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ya la libre circulación de estos datos.
- Constitución y definición de las funciones, del Comité de Firma Electrónica, órgano que asiste a la Comisión para todos los temas relacionados con la firma electrónica.
- Definición de los requisitos de los certificados reconocidos.
- Definición de los requisitos de los proveedores de servicios de certificación que expiden certificados reconocidos.
- Definición de los dispositivos seguros de creación de firma electrónica.
- Recomendaciones para la verificación segura de la firma.

Reglamento UE 910/2014, de 23 de julio	Sobre identidad electrónica y servicios de confianza para las transacciones electrónicas en el mercado interno
<ul style="list-style-type: none">• Establece en su Anexo II el valor como firma reconocida de las firmas emitidas utilizando mecanismos seguros de firma que no están bajo control físico directo del titular, sino gestionados por una entidad de confianza (repositorios HSM o similares).• Establece mecanismos para facilitar el reconocimiento transfronterizo de certificados electrónicos.	

Otros:

- Decisión 2002/20/CE, de 7 de marzo, sobre autorización de redes y servicios de comunicaciones electrónicas.
- Directiva 2002/58/CE, de 12 de julio, sobre tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas.
- Comunicación COM/567/2003, de 26 de septiembre, sobre el papel de la administración electrónica en el futuro de Europa.
- Dictamen de 16 de junio de 2004 respecto a la comunicación sobre el papel de la administración electrónica en el futuro de Europa.
- Comunicación COM/45/2006, de 13 de febrero, sobre interoperabilidad de los servicios paneuropeos de administración electrónica.
- Comunicación COM/173/2006, de 25 de abril, sobre el Plan de acción sobre administración electrónica i2010-Acelerar la administración electrónica en Europa en beneficio de todos.
- Comunicación de 23 de noviembre de 2006 sobre disposiciones relativas a la transmisión electrónica de las notificaciones de ayuda estatal.

- Decisión 2009/922/CE, de 16 de septiembre, sobre soluciones de interoperabilidad para las administraciones públicas europeas (ISA).

2.2 Estándares internacionales y otras convenciones

2.2.1 En materia de gestión documental

MoReq-2	Modelo de Requisitos para la Gestión de Documentos (Records) Electrónicos
<p>Norma para la gestión de archivos electrónicos, con una redacción que evita el lenguaje técnico. El principal uso de MoReq-2 está encaminado a la especificación y la compra de sistemas de gestión de archivos electrónicos.</p> <p>Elementos tratados en este modelo:</p> <ul style="list-style-type: none"> • Definición de modelos de metadatos (345 elementos diferentes). • Esquemas XML, para la gestión de archivos en un sentido amplio (Records Management). • Framework de prueba, para evaluar la idoneidad de las herramientas de gestión de archivos electrónicos. • Lista de requerimientos funcionales y no funcionales, a valorar. • Propone más de 800 requerimientos, de los cuales habrá que discernir los más adecuados en cada caso para obtener un modelo personalizado e idóneo para la Organización. • Otros temas: gestión de documentos y registros físicos, flujos de trabajo, integración con sistemas de gestión de contenidos (CMS), firma electrónica, cifrado.... • Existe una certificación MoReq-2 para productos de gestión de archivos electrónicos. 	

MoReq-2010	Revisión del Modelo de Requisitos para la Gestión de Documentos (Records) Electrónicos
<p>Esta norma desarrolla y actualiza el modelo tecnológico descrito en MoReq-2. Sin introducir cambios profundos en la filosofía de la gestión de recuerdos, adapta la arquitectura del sistema descrito en la evolución del contexto tecnológico:</p> <ul style="list-style-type: none"> • Describe un sistema más modular, donde las diferentes tareas especificadas dependen de sistemas separados pero interconectados. • Está muy enfocado a la interoperabilidad y el intercambio, para que los diferentes módulos puedan provenir de proveedores diferentes pero trabajar sobre los mismos objetos digitales. 	

ISO-15489 1/2	Información y documentación. Gestión de documentos archivo (Records Manager)
<p>Gestión de documentos de archivo por los sectores público y privado. Una metodología para la implantación de un programa de gestión documental en las empresas.</p> <p>Parte de la Norma Australiana AS 4390, Records Management.</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Definición de la importancia de las funciones y los elementos de los sistemas de gestión de documentos. • Define el mínimo común múltiplo de los países participantes. • Define algunos conceptos clave, que hay que tener presentes durante todo el documento, que se complica en las diversas traducciones nacionales, ya que dependiendo del país se puede entender una cosa u otra. Por ejemplo: recuerdo, recuerdos management,.... • Los metadatos asociados a un documento deberán contener: 	

1. La estructura de un documento, es decir, su formato y las relaciones entre los elementos que lo componen.
 2. El contexto de negocio donde el documento se ha creado, recibido y usado.
 3. Los vínculos entre documentos, que combinados forman un documento / registro.
- Establece que todos los documentos deben poder demostrar su autenticidad, fiabilidad, integridad y usabilidad.

ISO-23081 1/2	Procesos de gestión de documentos. Metadatos para la gestión de documentos
<p>Información y documentación. Procesos de gestión de documentos.</p> <p>Está compuesta por dos normas: en la primera que es del año 2006, se describen los principios que rigen esta temática. En la segunda, que data del año 2009, se hace un informe técnico incluyendo aspectos concretos de la implementación y conceptuales.</p> <p>Aspectos tratados en la ISO-23081-1 (2006):</p> <ul style="list-style-type: none"> • Perspectivas y utilidad de los metadatos para la gestión de documentos. • Roles y responsabilidades. • Gestión de metadatos. • Tipos de metadatos necesarios para implementar la norma ISO-15489-1. <p>Aspectos tratados en la ISO-23081-2 (2009):</p> <ul style="list-style-type: none"> • Objetivos y beneficios del uso de los metadatos. • Política y responsabilidades. • Modelo conceptual de metadatos. • Conceptos relacionados con la implementación de metadatos. • Desarrollo de un esquema de metadatos para la gestión de documentos. 	

ISO-26122	Análisis de los procesos de trabajo para la gestión de documentos
<p>Información y documentación. Análisis del proceso de trabajo para la gestión de documentos.</p> <p>Aspectos tratados en esta norma que data del año 2008:</p> <ul style="list-style-type: none"> • Inicio del análisis de los procesos de trabajo, y concretando con la dimensión documental de este análisis. Responsabilidades. • Estudio contextual. • Análisis funcional y secuencial. • Validar el análisis de los procesos de trabajo con los participantes. 	

ISO-30300 (2011)	Sistema de gestión para los documentos. Fundamentos y vocabulario.
<p>Norma que introduce toda la serie. Define la terminología que se utilizará en el resto de las normas de la serie y expone los motivos.</p>	

ISO-30301 (2011)	Sistema de gestión para los documentos. Requisitos.
<p>Es la norma que define los requisitos para la implantación de un sistema de gestión para documentos, sobre el que se harán evaluaciones y posibles certificaciones.</p> <p>Elementos tratados en estos estándares:</p> <ul style="list-style-type: none"> • Análisis previo. • Política, compromisos y roles. • Riesgos, objetivos y planes. • Recursos, formación y documentación. • Procesos y aplicaciones de gestión documental. 	

- Evaluación.
- Gestión de no conformidades, acciones correctivas y mejora continua.

ISO-16175-1 (2011)	Información y documentación. Principios y requerimientos funcionales para documentos en entornos de oficina electrónica. Parte 1: General y declaración de principios.
	<ul style="list-style-type: none"> • Buenas prácticas: documentos electrónicos y software • Principios rectores: relacionados con los documentos y con los sistemas. • Problemas de implementación: riesgos y mitigaciones; sostenibilidad financiera e institucional.

ISO-16175-2 (2011)	Información y documentación. Principios y requerimientos funcionales para documentos en entornos de oficina electrónica. Parte 2: Directrices y requerimientos funcionales para sistemas que gestionan documentos electrónicos.
	<ul style="list-style-type: none"> • Directrices: creación, mantenimiento, difusión y administración. • Requisitos funcionales: creación, identificación, clasificación, mantenimiento, acceso y seguridad, gestión de documentos híbridos, conservación y disposición, difusión y administración. • Lista de requisitos para la revisión de un sistema que gestiona documentos electrónicos.

ISO-16175-3 (2011)	Información y documentación. Principios y requerimientos funcionales para documentos en entornos de oficina electrónica. Parte 2: Directrices y requerimientos funcionales para documentos en sistemas de organización
	<ul style="list-style-type: none"> • Directrices para conservar la evidencia de los procesos. • Uso de los requisitos funcionales: creación, gestión y mantenimiento, soporte a la interoperabilidad y retención y disposición.

Otros:

- Consejo Internacional de Archivos, ISAD (G): Norma Internacional de Descripción Archivística, 2000, 2ª edición.
- Consejo Internacional de Archivos, ISAAR (CPF): Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y familias, 2004, 2ª edición.
- ISO 17933: 2000-GEDI-Generic Electronic Document Interchange. Intercambio genérico de documentos electrónicos.
- ISO / TS 20625. 2002-Intercambio electrónico de datos por administraciones, comercio y transporte (EDIFACT)-Rules for generation of XML schema files (XSD) on the basis of EDI (FACT) implementation guidelines.
- ISO 690-2-Información y documentación. Referencias bibliográficas. Parte 2: documentos electrónicos y partes de los mismos.
- UNE-EN ISO / IEC 17021:2011-Evaluación de la conformidad. Requisitos para los organismos que hacen auditoría y la certificación de sistemas de gestión.

2.2.2 En materia de firma electrónica

ETSI RFC 2315 (1998) ETSI RFC 2630 (1999) IETF RFC 3369 (2002) IETF RFC 3852 (2004)	PKCS # 7: Cryptographic Message Syntax (CMS)
--	---

Se utiliza para firmar digitalmente, obtener resúmenes de archivos, autenticar o cifrar mensajes.

Elementos tratados en este estándar / convención:

- Definición de la sintaxis general de datos que pueden tener criptografía asociada, como la firma digital.
- La sintaxis permite la recursividad, lo que permite, por ejemplo, que un sobre contenga otro.
- Definición del uso de atributos arbitrarios, como por ejemplo: instante de la firma, refrendo asociadas a una firma ...

ETSI TS 101 733 (2005)	Electronic Signatures and Infraestructuras (ESI); CMS Advanced Electronic Signatures (CAAdES)
-------------------------------	--

Elementos tratados en este estándar / convención:

- Definición de formatos de firma electrónica, incluidas las que pueden seguir siendo válidas a lo largo del tiempo, empleando pruebas respecto a su validez.
- Definición del concepto de política de firma electrónica, que establece la consistencia técnica.
- Convención del uso de sello de tiempo (time-stamping) y servicios de marcación de tiempo, necesarios para probar la validez de la firma a largo plazo.

IETF RFC 5280 (2008)	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
-----------------------------	---

Forma parte de la familia de estándares relacionados con X.509 Public Key Infrastructure.

Elementos tratados en este estándar / convención:

- Definición de las especificaciones a cumplir por las CRLs (listas de revocación de certificados).
- Definición de los procedimientos de validación con la correspondiente ruta de certificación.

IETF RFC 2560 (1999)	X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP
-----------------------------	--

Protocolo utilizado para determinar el estado actual de un certificado digital sin necesidad de CRLs.

Elementos tratados en este estándar:

- Definición del protocolo para determinar el estado de los certificados digitales.
- Definición de los OCSP sobre HTTP.
- Acumulación de elementos sintácticos ASN.1.
- Especificación de los tipos MIME para los mensajes.

ETSI TS 101 903 (2006)	XML Advanced Electronic Signatures (XAAdES)
-------------------------------	--

Elementos tratados en este estándar:

- Definición de nuevos tipos de XML con nuevas propiedades que califican las firmas XMLDSIG con información adicional, como la validez a largo plazo de la firma para el uso de sello de tiempo. Especificación de cómo incorporar esta información al objeto digital.

- Definición de dos tipos principales de propiedades: las firmadas y las no firmadas. El primer tipo es opcional y quedarán securizados mediante la firma del signatario. Las propiedades no firmadas son agregadas por el firmante, por el verificador, o por otras partes después de la producción de la firma.

2.2.3 En materia de digitalización e impresión segura

Resolución de 19 de julio de 2011 , de la Secretaría de Estado para la Función Pública	Norma Técnica de Interoperabilidad de Digitalización de Documentos
Elementos tratados en esta NTI: <ul style="list-style-type: none"> • Requisitos técnicos y procedimentales para la digitalización de documentos con validez jurídica. • Formato de los documentos electrónicos resultantes, tanto en cuanto a formato de documento digital como representación de los metadatos asociados al proceso de digitalización. • Requisitos de calidad de la imagen electrónica. 	

ISO 12651 (1999)	Recomendaciones para la creación de documentos originales
El objetivo principal de este estándar es facilitar la comunicación en el campo de la imagen electrónica. Elementos tratados en este estándar: <ul style="list-style-type: none"> • Vocabulario • Escáneres ópticos • Ópticos de almacenamiento • Procesamiento de imágenes (ordenador) • Procesamiento de datos • Gráficos por ordenador • Equipos periféricos • Escáner (ordenadores) • Métodos de grabación digital 	

ISO 12652	Informe técnico sobre la preparación de los documentos para los sistemas de captura de imágenes
Este estándar se divide en dos partes: en la primera se tratan las características de la captura y en la segunda el método empleado para hacerlo.	

ISO 12653 (2000)	Imágenes electrónicas - Prueba de resultados de la digitalización de documentos de oficina en blanco y negro
Planificar la preparación de documentos para ser digitalizados, los sistemas de captura de imagen.	

ISO 10196 (2003)	Recomendaciones para la creación de documentos originales
Proporciona directrices para la creación de documentos originales para facilitar su reproducción como microformas. Esta norma se aplica a documentos en negro sobre un fondo claro,	

constituidos por líneas continuas. Aunque los estudios se basaron más específicamente en el alfabeto latino, los principios generales pueden servir como directrices para la producción de documentos que utilizan otros alfabetos o ideogramas.

ISO 15801 (2004)	Imágenes electrónicas - Información almacenada electrónicamente
<p>Recomendaciones para garantizar la integridad y la fiabilidad de la información almacenada.</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Implementación y definición del funcionamiento de los sistemas de gestión de la información que la almacenan en forma electrónica y donde las cuestiones de fiabilidad, autenticidad y la integridad son importantes. • Cubre el ciclo de vida completo de un documento electrónico almacenado, desde la captura inicial hasta la eventual destrucción. • Definición de los requisitos necesarios, para poder demostrar que la salida del sistema es una reproducción fiel del documento original. 	

Otros:

- Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación.
- Resolución de 24 de octubre de 2007, de la Agencia Estatal de Administración Tributaria, sobre el procedimiento para la homologación de software de digitalización contemplado en la Orden EHA/962/2007, de 10 de abril de 2007.
- ISO 11506: 2009-Document management applications-Archiving of electronic data-Computer output microform (COM) / Computer output laser disc (COLD).
- UNE-ISO/TR 13028: 2010 - Información y documentación. Directrices para la implementación de la digitalización de documentos.
- UNE-ISO/TR 13008: 2010 - Información y documentación. Conversión de documentos digitales y procesos de migración.

2.2.4 En materia de preservación del documento electrónico

IETF RFC 3126 (2001)	Electronic Signature Formats for Long Term Electronic Signatures
<p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Definición del formato de la firma electrónica para que siga siendo válida a lo largo del tiempo, incorporando pruebas que no permitan la posterior negación por parte del firmante. • Definición de una estructura de firma electrónica que proporciona las correspondientes evidencias para obtener la confianza de que existe un compromiso explicitado bajo una política de firma. • Especificación del uso de los proveedores de servicios de confianza (Time Stamping Authorities). • Correspondencia de contenido con la convención publicada por ETSI TS 101 733. 	

ISO 14721 (2003)	Modelo de referencia OAIS
<p>Space data and information transfer systems - Open archival information system (OAIS).</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Definición de un modelo de archivo de documentos electrónico, con el objetivo de garantizar la disponibilidad de la información en todo momento, sobre todo a lo largo del tiempo. • Su funcionamiento se basa en tres procedimientos muy concretos: incorporación, archivo y disposición. • Centrado con la información digital como forma primaria de la información y como información de apoyo de los materiales archivados. • Las directrices del modelo se han definido desde un prisma de voluntad y filosofía de trabajo abierta, tendiendo al acceso libre sin restricciones, salvo las necesarias a nivel de control de acceso. 	

ISO 18492 (2008)	Conservación de documentos a largo plazo
<p>Conservación a largo plazo de la información basada en documentos.</p> <p>Aspectos más importantes:</p> <ul style="list-style-type: none"> • Estrategia de conservación a lo largo del tiempo. • Renovación de los soportes. • Metadatos de preservación. • Migración de la información electrónica, basada en documentos. • Política de preservación a lo largo del tiempo. • Control de calidad. • Seguridad. 	

ISO 19005 (2008)	Formato de archivo PDF/A-1
<p>Gestión de documentos. Formato de archivo de documento electrónico para la conservación a lo largo del tiempo. Parte 1: Uso del PDF 1.4 (PDF/A-1).</p> <p>Niveles de conformidad.</p> <p>Requisitos técnicos: estructura del archivo, gráficos, fuentes, transparencia, anotaciones, acciones, metadatos, estructura lógica y formularios interactivos.</p>	

ISO 15801 (2004)	Documentos electrónicos. Almacenamiento electrónico de informaciones. Recomendaciones para garantizar la veracidad y fiabilidad de los documentos
<p>Electronic imaging-Information stored electronically-Recommendations for trustworthiness and reliability.</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Definición de las condiciones requeridas para garantizar la veracidad, fiabilidad, autenticidad e integridad de los documentos en el marco de un sistema de gestión de expedientes electrónicos. • Se ocupa de dictar especificaciones referidas a los tipos de documentos afectados, los medios de almacenamiento, los formatos y el control de versiones, la gestión de estándares, las políticas de retención y destrucción. • Define la responsabilidad para gestionar la información y para auditar su grado de cumplimiento. • Da directrices referidas a la captura de documentos, digitalización, inserción de metadatos, indexación, procedimientos de autenticación, la transferencia de expedientes, la retención y destrucción de información, los back-ups, y sistemas de seguridad, el 	

mantenimiento del sistema , la seguridad y protección, la gestión de workflows, los sellos de tiempo y el control de versiones.

- En cuanto a la plataforma tecnológica, especifica puntos a tener en cuenta: Plan de sistema, medios de almacenamiento, niveles de acceso, verificación de la integridad del sistema, migración y supresión de información.

ISO 20652 (2006)	Repositorios digitales y sistemas de transferencia de información. Productor-Archivo. Metodología de transferencia estándar.
<p>Space data and information transfer systems-Producer-archive interface-Methodology abstract standard ..</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Definición de una metodología para formular modelos de relación entre los productores de objetos digitales y los repositorios electrónicos de archivos generados de acuerdo con la norma OAIS. • Define las tareas a desarrollar y las condiciones de seguridad requeridas en todo el proceso de transferencia de los objetos digitales al repositorio electrónico de archivo. • Permiten valorar eficiencias en casos de aplicación práctica. 	

Otros:

- ISO / TR 18492: 2005 - Long-term preservation of electronic document-based Information.

2.2.5 En materia de seguridad

ISO / IEC 15816 (2002)	Tecnología de la información - Técnicas de seguridad - Información de seguridad para los objetos de control de acceso
<p>Las técnicas de seguridad intentan garantizar que los activos, incluida la información, están protegidos de manera adecuada y rentable. La gestión de la información de la organización es muy importante, para proteger los intereses de propiedad y derechos de propiedad intelectual.</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Definición de directrices para la especificación de la sintaxis abstracta de genéricos y específicos de Seguridad de los objetos de información (SIO) para control de acceso. 	

ISO / IEC 17799 (2005)	Tecnología de la información - Técnicas de seguridad - Recomendaciones prácticas para la gestión de seguridad de la información
<p>Establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.</p> <p>Elementos tratados en este estándar:</p> <ul style="list-style-type: none"> • Describe mejores prácticas (Best practices) de los objetivos de control y los controles, en el área de gestión de la seguridad de la información, mediante: <ol style="list-style-type: none"> 1. Políticas de Seguridad. 2. Organización de la información de seguridad. 3. Gestión de activos. 4. Seguridad de recursos humanos. 5. Seguridad física y ambiental. 6. Gestión de comunicaciones y operaciones. 7. Control de acceso. 8. Adquisición, desarrollo y mantenimiento de sistemas de información. 9. Gestión de la información de incidentes de seguridad. 	

- | |
|--|
| 10. Gestión de continuidad del negocio.
11. Conforme con el marco actual. |
|--|

ISO / IEC 18028 (2006)	Tecnología de la información - Técnicas de seguridad - Seguridad de Red TI
Este estándar está dividido en varias partes: <ul style="list-style-type: none">• Parte 1: Gestión de la seguridad de la red.• Parte 2: Arquitectura de la seguridad de la red.• Parte 3: Asegurando las comunicaciones entre redes que utilizan gateways de seguridad.• Parte 4: Asegurando el acceso remoto.• Parte 5: Asegurando las comunicaciones entre redes utilizando redes privadas virtuales.	

ISO / IEC 27001 (2005)	Seguridad en las Tecnologías de la información.
Information technology-Security techniques-Information security management systems-Requirements.	
Elementos tratados en este estándar: <ol style="list-style-type: none">1. Autenticidad.2. Irrefutabilidad.3. Integridad.4. Confidencialidad.5. Disponibilidad.6. Criticidad.7. Cumplimiento legal.	

Otros:

- RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

3. El sistema de gestión documental y el ciclo de vida de los documentos

3.1 Introducción

Es importante remarcar que todo sistema de gestión de documentos formula una metodología que puede ser aplicada de manera indistinta a documentos en soporte en papel o en soporte electrónico, y que los instrumentos técnicos que debe generarse en cualquier caso se fundamentan en la normativa internacional sobre gestión documental. La asunción de la gestión de documentos electrónicos como una función netamente archivística y como una instrumentación directa de los SGD viene avalada por las tres grandes disposiciones normativas como son las familias de normas ISO 15489, 30300 y 16175. Y en la misma línea se expresan las normas emanadas del Consejo Internacional de Archivos. En el momento de generarse un documento un elemento capital es su carácter de prueba de derechos y obligaciones en la medida que se insertan en el marco de procedimientos administrativos, más allá del soporte en que se refleje.

Otra cuestión es que la producción de documentos electrónicos confiere a los valores clásicos de autenticidad, integridad, fiabilidad y usabilidad un carácter central y una necesidad de cumplimiento ineludible para garantizar su validez procedimental y legal. O dicho de otra manera, elementos que en un soporte en papel podían cumplirse con una cierta facilidad –autenticidad mediante firma manuscrita o sellos institucionales, accesibilidad directa mediante lectura sin intermediaciones, durabilidad ligada únicamente a la solidez del soporte- devienen más complejas en el documento electrónico y precisan del recurso imprescindible a la firma electrónica, el manejo del hardware y el software adecuado y una clara estrategia de preservación a largo plazo.

Asimismo, la facilidad de “manipulación” del documento electrónico ha propiciado un cierto cambio en la percepción y uso de los documentos en sus fases de trámite y vigencia. En poco tiempo la literatura científica en gestión de documentos ha asumido que el documento, con anterioridad percibido como una unidad estática desde su generación, alcanza una nueva dimensión en su vertiente electrónica; de esta manera se usa crecientemente –fundamentalmente por influencia de la MoReq2- los términos “documento de gestión”, ubicado en la fase de trámite y sometido a cambios continuados y el documento de archivo o record, para evidenciar la aprobación formal del expediente y su carácter inalterable al pasar a la fase de vigencia.

Así, a lo largo de los siguientes epígrafes presentamos un breve análisis de la situación actual y se describe el ciclo de vida y sus componentes más relevantes que constituyen la parte nuclear del protocolo: el modelo de información, la incorporación de los documentos al sistema y su registro, la clasificación de los documentos y el catálogo de tipologías documentales, la evaluación, disposición, retención y calendario de conservación, la clasificación de seguridad y acceso, el almacenaje, la preservación a largo plazo y la firma electrónica, la digitalización certificada e impresión segura, las evidencias electrónicas y la trazabilidad, y un capítulo que contiene un glosario básico.

Cabe señalar que algunos aspectos decisivos para la plena conformación de un SGD – digitalización, acceso y seguridad, metadatos, preservación digital y firma electrónica – los hemos tratado de manera muy sintética ya que son objeto de un tratamiento más exhaustivo en la segunda parte de este proyecto.

3.2 Alcance del modelo documental

El modelo de gestión documental es el reflejo de una política consistente en el establecimiento de un conjunto de directrices, procedimientos, prácticas y normas para garantizar la gestión de los expedientes a lo largo de todo su ciclo de vida, con la finalidad de gestionar documentos auténticos, fiables, íntegros y accesibles. En este sentido, los requerimientos y recomendaciones que se plantean en este protocolo son de aplicación obligada al Ayuntamiento de Pamplona y sus entidades vinculadas y afecta a la totalidad de su personal, tanto de plantilla como contratado, sea en grado de dependencia directa de la institución o a través de empresas externas mediante convenio.

Asimismo, el modelo de gestión documental debe aplicarse a todos los documentos en cualquier soporte (papel o electrónico) creados o recibidos por el Ayuntamiento y entidades vinculadas en la medida que son testimonio y evidencia de sus actividades, más allá de su fecha de creación. En concreto, el modelo tiene la vocación de implementarse sobre los siguientes tipos de documentos:

- Documentos textuales, en soporte papel o electrónico
- Documentos en imagen (fija o en movimiento)
- Documentos figurativos (gráficos, cartográficos e iconográficos)
- Documentos sonoros (grabaciones institucionales y testimonios orales)

A su vez, el alcance del modelo implica también no sólo a los documentos generados por el Ayuntamiento y entidades afines, sino también a todos aquellos documentos, expedientes y fondos ingresados a la institución vía cesión, donación o compra procedente de entidades o personas privadas (fondos personales, de entidades y asociaciones y de empresas).

3.3 Ciclo de vida de los documentos

La gestión adecuada de los documentos y de la información que generan las organizaciones constituye un reto en la medida en que su resolución asegura la calidad de las decisiones adoptadas, garantiza la eficacia y la eficiencia de los procesos e incide en la mejora de la productividad. Por estas razones las organizaciones impulsan la implantación de sistemas de gestión documental corporativa mediante la interacción entre las herramientas tecnológicas y las normas y directrices técnicas de la gestión de los documentos y los archivos.

Como preceptúa la norma ISO 30300: 2011 (2.3.1), el objetivo de implementar un SGD es crear y controlar documentos de una manera sistemática y verificable con la finalidad de:

- Llevar a cabo las actividades de la organización y prestar los correspondientes servicios de manera eficaz;
- Cumplir con los requisitos legislativos, reglamentarios y de rendición de cuentas;
- Optimizar la toma de decisiones, la consistencia operativa y la continuidad del negocio;
- Facilitar el funcionamiento efectivo de una organización en el caso de desastre;
- Proporcionar protección y soporte en los litigios, incluyendo la gestión de riesgos asociados con la existencia o no de pruebas de una actividad organizativa;
- Proteger los intereses de la organización y los derechos de los empleados, los clientes y las partes interesadas actuales y futuras;
- Dar apoyo a las actividades de investigación y desarrollo;
- Apoyar las actividades promocionales de la organización; y
- Mantener la memoria corporativa o colectiva y apoyar la responsabilidad social.

Un elemento capital y que influye sobre todo el proceso de gestión documental es la exigencia de fiabilidad, autenticidad, integridad y usabilidad de los documentos electrónicos por parte de la legislación española y la normativa internacional. Estos factores de validez conllevan unos requerimientos de gestión con respecto a su captura, registro, descripción, clasificación, utilización, localización y disposición (conservación o eliminación, en su caso). En este ciclo de vida de los documentos hay un cierto consenso en admitir la existencia de tres fases relevantes:

- La fase de tramitación, también denominada fase activa, que se extiende desde la creación o ingreso del documento o expediente hasta su aprobación formal. En el aspecto tecnológico se trabaja con aplicaciones departamentales y herramientas de gestión de procesos (BPM - Business Process Management), pensados especialmente para la definición, ejecución y control de las tramitaciones de las áreas del Ayuntamiento.
- La fase de vigencia, o fase semiactiva, durante la cual el expediente es necesario para la gestión administrativa y como referencia legal y testigo perdurable de los actos de la organización.
- La fase histórica o de conservación permanente, en la cual se procede a la conservación y uso de los documentos de carácter informativo y de valor relevante para la investigación que devienen el patrimonio documental de la organización.

La especificidad de las dos primeras fases y las diferencias en su tratamiento y uso, no exime de la necesidad imperiosa de impulsar un tratamiento estandarizado de los documentos / expedientes hasta su ingreso en el área de Archivo (fase histórica o de

conservación permanente). Para alcanzar una continuidad en la gestión a lo largo del ciclo de vida hay que consolidar una arquitectura de sistemas que se concreta en la utilización sucesiva de herramientas y programas de gestión documental (DM - Document Management) y del ciclo de vida (RM - Record Management).

3.4 Modelo propuesto

3.4.1 Fase de tramitación:

Los documentos y expedientes se incorporan al Sistema de Gestión de Documentos en la fase de tramitación, durante la cual son utilizados para plasmar las actuaciones y soportar las decisiones que componen un procedimiento administrativo.

- Excepcionalmente se pueden incorporar al SGD unidades documentales procedentes de la cesión de otros fondos documentales. En estos casos, los documentos no corresponden a trámites en curso y por tanto se incorporan al SGD directamente en fase histórica.

La incorporación del documento, por tanto, se produce mediante la captura, que se comentará en mayor detalle en el apartado 3.4.1.

La gestión de los documentos durante la fase de tramitación se caracterizará por:

- a) El área o departamento responsable del trámite es también responsable del expediente y de la documentación que lo compone. Esta no quita que las competencias para determinar las políticas de gestión documental, así como cualquier decisión sobre la eliminación de documentos, compiten al Archivo General.
- b) Los derechos de acceso a la documentación se definen en base a la necesidad de poder tramitar ágilmente el procedimiento asociado.
- c) El expediente se va componiendo progresivamente a medida que se añaden documentos a él.
- d) La incorporación de un documento implica los procesos de **captura, registro, clasificación y descripción**, tal como se detallarán más adelante. Es crítico, en esta fase del procedimiento, garantizar que los mecanismos de captura permitan una clasificación y descripción precisa y eficiente, automatizada al máximo posible para evitar la sobrecarga de las personas responsables de la tramitación.

Los documentos que se incorporan al SGD provenientes de fuentes externas deben además registrarse en el **registro de entrada de documentos del Ayuntamiento**, acción que implicará:

- Incorporar los datos descriptivos de la unidad documental, de acuerdo con el modelo de descripción y metadatos básicos.
- Identificar la tipología documental, de acuerdo con el catálogo de tipologías del Ayuntamiento.
- Determinar la ubicación del documento en el Cuadro de Clasificación:
 - Si el documento va asociado a un expediente existente, queda clasificado mediante su asignación a dicho expediente.
 - Si el documento provoca la creación de un nuevo expediente, dicho expediente se deberá clasificar adecuadamente.
 - Si no se puede conocer a priori el tipo de expediente al que pertenece el documento, se ubicará provisionalmente en una carpeta temporal, sobre la que existirá un estricto control para evitar que los documentos queden suspendidos sin asociarse a acciones concretas.
- Asignación de roles y permisos, de manera implícita por la clasificación documental.

Registro general de expedientes: Todo expediente de nueva creación se debe crear a través de este registro, que asignará un identificador único al expediente, creará la unidad documental compuesta correspondiente y registrará la información relativa a:

- a. Código del expediente
- b. Código de clasificación
- c. Título del expediente

Este registro permite disponer de la información básica sobre todos los expedientes que se tramitan en la casa, garantiza la unicidad de la numeración y permite definir políticas de acceso en función de la tipología del expediente.

Cualquier documento del Ayuntamiento deberá pertenecer a un expediente desde su creación, y los que se reciban a través del registro general de entrada deberán ser asignados a uno tan pronto como se haya tenido ocasión de analizar su contenido.

Los documentos que se incorporan a un expediente reciben una numeración secuencial a medida que se van incorporando, que puede ser proporcionada de manera automática por la plataforma informática, y que tiene como finalidad garantizar la integridad del conjunto y preparar el futuro foliado.

3.4.2 Fase de vigencia:

Una vez finalizado el procedimiento y aprobado por el órgano competente, importa asegurar la continuidad y perdurabilidad de la información incorporada. En esta fase, el

tratamiento de los documentos y expedientes es competencia del Archivo General, y sus responsabilidades se centran en los procesos siguientes:

- a) **Formalización de la transferencia:** El Archivo define el formulario de transferencia a través del cual el departamento responsable debe confirmar el cambio de fase del expediente en el momento de cerrarlo. Esta acción comporta el cierre del expediente y el cambio de permisos de acceso. La introducción de este mecanismo ha de permitir controlar que los expedientes estén correctamente formados antes de trasladar las competencias sobre su gestión.

Cabe observar que se producen algunos cambios respecto a la operativa en papel, ya que la transferencia se decide expediente por expediente, y no mediante remesas. El Archivo deberá organizarse para revisar y aceptar las transferencias con la periodicidad adecuada.

Un expediente cuya transferencia haya sido solicitada pero aún no autorizada, se considerará en fase de vigencia a efectos de permisos de acceso, pero no quedará cerrado ni se foliará e indexará en tanto no se realice la revisión pertinente. La revisión puede comportar, en caso de que se detecten defectos, la reversión a la fase activa para, una vez subsanados, ser completados.

Con la finalidad de garantizar que la transferencia se produce cuando corresponde, se debe definir un mecanismo a través del cual se detecten aquellos casos de expedientes abiertos que permanezcan durante un periodo excesivo sin actividad. En estos casos se comunicará la situación tanto al responsable del expediente como al archivo para su revisión.

- b) **Control de formatos (Catálogo de formatos):** Los documentos que componen el expediente deberán en todo caso responder a formatos aptos para el archivo a largo plazo, de acuerdo con lo que se establezca en las instrucciones correspondientes.
- c) **Políticas de conservación:** El Archivo iniciará la aplicación de las Tablas de Evaluación Documental, una vez efectuada la transferencia.
- d) **Política de seguridad y acceso:** Durante esta fase, los expedientes pueden ser consultados directamente por el departamento responsable de su elaboración o ejecución. Otros interesados sólo podrán acceder a consulta previa autorización del Archivo.
- e) **No modificabilidad:** Los expedientes en fase de vigencia no pueden ser modificados, excepto en casos excepcionales, en los que, bajo la supervisión del Archivo, se autorizará la reapertura del expediente sólo a efectos de agregar documentos, extremo que quedará garantizado mediante la conservación del índice previo junto con el índice más reciente.

3.4.3 Fase histórica

Los expedientes entrarán en esta fase, transcurridos los plazos de vigencia que establezcan las Tablas de Evaluación Documental. En esta fase interesa preservar el valor de los documentos como testimonio histórico de la actividad de la organización, por lo que se aplican las siguientes medidas:

- a) Completar la descripción del expediente con la información pertinente de carácter archivístico, si corresponde.
- b) Aplicación de las políticas de conservación de acuerdo con lo que se prevea para esta fase.
- c) En relación a expedientes híbridos u otros documentos que aún se encuentren en soporte papel, puede corresponder la aplicación de las políticas de digitalización, en función de la importancia de los documentos o expedientes.
- d) Se debe formalizar la transferencia, lo que puede implicar un componente físico, dado que los documentos en fase histórica podrían ubicarse en un repositorio digital seguro orientado a la preservación a largo plazo, distinto del resto de herramientas del Ayuntamiento.

3.5 Los procesos de gestión de documentos del sistema

La metodología de gestión de los documentos y archivos ha integrado las recomendaciones emanadas de los organismos internacionales (Consejo Internacional de Archivos, Unión Europea) y muy especialmente las directrices derivadas de las normas ISO referidas a gestión documental, procesos, preservación, metadatos, digitalización y seguridad. También inciden en las posibles soluciones las formulaciones contenidas en el Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI). A partir de estos referentes normativos los expertos en gestión de documentos y archivos han asumido una serie de convenciones metodológicas e instrumentales que deben permitir una actuación concertada que asocie la tecnología con la metodología adecuada para garantizar un tratamiento homogéneo a lo largo de todo el ciclo de vida de los documentos.

De acuerdo con estos antecedentes, se definen fundamentalmente ocho procesos fundamentales en la gestión de documentos, según se detalla a continuación:

1. **Captura de los documentos** (manual, automática o mediante digitalización certificada). Esta captura conlleva un proceso de registro, de cambio de espacio lógico y de asignación de permisos.
2. **Registro:** se genera una breve descripción a nivel de unidad documental (identificador único, fecha y hora, título o descripción y órgano).
3. **Clasificación de los documentos** (Funcional, de seguridad y acceso). Esta estructura sirve de base para establecer las políticas de acceso y seguridad.

4. **Descripción de los documentos:** Aplicación de las normas de descripción normalizada internacional y, muy especialmente, del modelo de metadatos.
5. **Almacenamiento, preservación a largo plazo y firma electrónica,** especialmente para los documentos con valor de evidencia.
6. **Disposición, retención y calendario de conservación.** Conservación y eliminación de documentos con especial atención a la aplicación de los calendarios de conservación.
7. **Transferencia de los documentos:** Garantizar la continuidad del ciclo de vida mediante la transferencia física o telemática en las tres fases de los documentos
8. **Uso, consulta, impresión segura y trazabilidad:** control de acceso y permisos, registros de auditoría, control de versiones y mecanismos de seguridad.

Al tratar la gestión de documentos electrónicos, nos encontramos con que la capacidad para automatizar determinados procesos permite, sin dejar de destacar la importancia individual de cada uno de ellos, agruparlos por unidad de acción en la operativa del documento electrónico. A continuación, individualizamos los momentos clave en la tramitación de un expediente en soporte electrónico.

3.5.1 Incorporación de los documentos al sistema: producción, captura y registro de documentos

Las normas internacionales y, más concretamente, la norma ISO 30301:2011 determinan los requerimientos para la creación, captura, registro y gestión de documentos con la finalidad que puedan cumplir con las necesidades de información en relación con los procesos de la organización, en este caso, el Ayuntamiento. Dado que el establecimiento, implementación y mantenimiento de un SGD se inicia en el momento de la creación o captura de los documentos, es necesario establecer de manera planificada la manera en que se generarán o recuperarán los documentos según sean presentados por los ciudadanos o bien generados por el propio Ayuntamiento en aplicación de algún trámite administrativo.

En este contexto, y en el marco de la gestión de documentos electrónicos, es necesario proceder a planificar los elementos básicos para alcanzar unos procedimientos conformes a la legalidad y, sobre todo, a su valor de evidencia. Es imprescindible ejecutar un control de los documentos que se plasma en el diseño normalizado de documentos (formularios), la integración del catálogo de tipologías documentales en la medida que conforman de manera armónica el expediente electrónico, y especialmente el estudio de los circuitos administrativos que frecuentemente conlleva una reingeniería de procesos.

Por lo que se refiere a la captura de documentos físicos o electrónicos, la norma ISO 15489-1: 2001 (sección 9.3) establece que su finalidad es asegurar el establecimiento de una relación efectiva entre el documento, su productor y el contexto de producción, de manera

que sitúe el documento en el sistema de gestión y permita asociarlo a otros documentos. A su vez, la citada ISO 30301 señala que se deben identificar y documentar los métodos de integración de captura de documentos en los procesos de negocio (A.1.1.6), integrar y documentar la información descriptiva y de contexto necesaria para identificar los documentos en cada proceso de trabajo (A.1.2.1) y finalmente se deben identificar en los procedimientos para cada proceso de trabajo los momentos en que se captura la información contextual o en que se añade a los documentos y sus fuentes (A.1.2.2).

En su vertiente legal y de gestión, remarcar que el registro de entrada es el primer paso del proceso de incorporación, tal como señala la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en su artículo 38.4 y, a partir del 2 de octubre de 2016, la ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas en su artículo 16.

Modelo propuesto

Atendiendo a los antecedentes expuestos y a las particularidades de la documentación administrativa, distinguimos cuatro casos distintos de captura de documentos, que comentamos a continuación:

- a) **Producción interna original electrónica:** La fortaleza de un SGD radica en su capacidad para potenciar la creación de documentación original en forma electrónica de manera que su inserción al sistema sea rápida y eficiente.

La documentación que nazca en formato electrónico dentro de los sistemas del Ayuntamiento deberá respetar los siguientes principios básicos:

- Se deberá garantizar el cumplimiento del catálogo de formatos de acuerdo con las directrices contenidas en el protocolo correspondiente.
- A menudo los documentos provendrán de herramientas de gestión que normalmente tienen acceso a un gran volumen de información. Se deberá aprovechar esta circunstancia para alimentar el máximo de metadatos de manera automática.
- La autenticidad de los documentos deberá quedar acreditada mediante:
 - O bien una firma electrónica que cumpla con todos los requisitos de seguridad y formato que establezca la política de firma electrónica del Ayuntamiento,
 - O bien mediante alguna evidencia del sistema que acredite que el documento se ha generado conforme a lo que exija la normativa aplicable.

b) **Recepción de documentación original electrónica:** En este caso estamos previendo la circunstancia en la que los interesados en los procedimientos aportan al Ayuntamiento documentación electrónica. Es de prever que éste sea el modelo de captura que tenga un mayor crecimiento en el futuro. En estos casos es importante tener en cuenta que:

- Al tratarse de documentación de origen externo, deberá anotarse en el registro de entrada, a través de la integración del registro de entrada telemático.
- La anotación en el registro de entrada implica la incorporación de una serie de datos, que serán informados por el usuario externo y deberán incorporarse como metadatos. Para evitar problemas de integridad y consistencia, es importante, por tanto:
 - Ofrecer al usuario externo todas las facilidades para normalizar los datos que incorpore.
 - Introducir mecanismos para validar o confirmar aquellos datos sobre los que se puedan producir errores al introducirlos.
- En relación al formato del documento, se deberá comprobar en este momento que responde a uno de los formatos admitidos en el catálogo del Ayuntamiento.
- El documento de origen externo puede tener que ir firmado electrónicamente, en cuyo caso la firma será validada y completada con sello de tiempo en el momento de la recepción, conforme se establece en la política de firma electrónica del Ayuntamiento.

c) **Digitalización de documentación original en papel:** Aplica al caso de captura de documentos físicos, sean generados por los ciudadanos o por el propio Ayuntamiento. La conversión de documentos analógicos en documentos electrónicos se lleva a cabo mediante la digitalización del documento original de acuerdo con lo que establezca el Modelo de Digitalización de documentos del Ayuntamiento, que atenderá, entre otros condicionantes, las prescripciones contenidas en el Esquema Nacional de Interoperabilidad, la Ley 11/2007 y, a partir del 2 de octubre de 2016, la ley 39/2015.

El Modelo de Digitalización de Documentos deberá contemplar cuestiones como:

- Diferentes escenarios de digitalización: compulsa a la entrada, digitalización interna, digitalización automatizada y externalización del proceso.
- Diferentes niveles de seguridad: obtención de imagen electrónica con carácter de copia simple, u obtención de copias auténticas mediante digitalización certificada, que permiten la sustitución del soporte papel.
- Metadatos e información contextual adicional que se deberá capturar para registrar las particularidades del proceso de conversión.

No todos los documentos que se reciben en papel deben ser digitalizados. Puede darse el caso de que haya documentos cuya digitalización no sea necesaria o recomendable, lo que podría dar lugar a la existencia de expedientes híbridos, que contendrían documentación electrónica junto con elementos en papel, los metadatos de los cuales se incorporarían igualmente al expediente electrónico.

- d) **Documentos obtenidos mediante mecanismos de interoperabilidad:** Finalmente, existirán documentos que el Ayuntamiento obtendrá no por ser aportados por un interesado, sino por intercambio de datos e información con otras administraciones dentro del ejercicio de sus funciones. Estos documentos se crearán de acuerdo con los criterios que establecen las Normas Técnicas de Interoperabilidad, según las interpreten los organismos productores. El Ayuntamiento deberá estar preparado para acceder a estos documentos e incorporarlos a sus expedientes electrónicos, realizando las acciones necesarias para garantizar la validez de sus firmas electrónicas, según se detallará en el documento de política correspondiente.

3.5.2 Clasificación de los documentos

De acuerdo con la norma ISO 15489 la clasificación es *“la identificación y estructuración sistemática 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 cuadro de clasificación”*. La construcción del Cuadro de Clasificación supone integrar en un instrumento sistemático un conjunto de informaciones derivadas de un análisis de la historia de la institución, la estructura y funciones del organismo, la identificación de la producción documental, el marco legal y jurídico, la compilación de clasificaciones históricas y el conocimiento exhaustivo de los procedimientos administrativos.

Ante la tendencia consolidada durante la segunda mitad del siglo XX de creer que la peculiaridad o carácter distintivo de un Cuadro de Clasificación en relación a otros le confería un plus de calidad, debemos manifestar explícitamente que para los documentos administrativos es básico elaborar un cuadro de carácter funcional. Se trata de un sistema de clasificación basado en una estructura jerárquica y lógica que refleje las funciones y actividades de una organización. La consolidación de las competencias y funciones – generando así series documentales estables y continuas-, la solidez alcanzada en el régimen jurídico de las administraciones y la creciente formación del personal de oficinas reafirman el papel protagonista de este modelo de clasificación. En todo caso, el intenso cambio en los organigramas de las corporaciones hace absolutamente inviable aplicar cuadros de clasificación orgánicos, actualmente limitados a los fondos históricos que mantienen una clasificación de origen.

Para la construcción del Cuadro de Clasificación nos remitimos a la Norma Internacional para la descripción de funciones (ISDF) que se basa en el principio que el análisis de las

funciones de las instituciones debe convertirse en la base para muchas de las actividades de la gestión de documentos. Cabe señalar que la correcta identificación de las funciones y su desarrollo, y su relación con la producción documental (fondo, serie, expediente y unidad documental simple) deviene la clave de bóveda del cuadro de clasificación. En todo caso, tanto los planteamientos de la norma ISDF como la propuesta del Esquema nacional de Interoperabilidad, los conceptos de fondo, serie, expediente y unidad documental simple constituyen el armazón estructural de los cuadros de clasificación de carácter funcional.

La tendencia internacional es adaptar los cuadros de clasificación de tipo funcional a la estructura de procedimientos y procesos de las organizaciones mediante un desarrollo superior de los niveles funcionales mediante la inserción de procedimientos y procesos de gestión en base a la secuencia: función/actividad/transacción/serie documental. Este planteamiento, en sintonía con las disposiciones contenidas en las ISO 15489-2 y 16175-3, recomienda la construcción de un Cuadro de Clasificación funcional de tres niveles como mínimo y que concretan de la siguiente manera:

- Nivel 1: **función de negocio**. Serie. Constituida por agrupaciones de documentos que pueden denominarse “clase” o “categoría”.
- Nivel 2: **actividad**. Expedientes, que constan de agrupaciones individuales que pueden denominarse “carpetas” o “contenedores”. Se pueden subdividir en volúmenes.
- Nivel 3: **operación**. Documentos. Pueden estar formados por diferentes componentes.

En el caso del Ayuntamiento de Pamplona, una vez analizados diferentes modelos implantados en varios ayuntamientos españoles, se ha procedido a construir un Cuadro de Clasificación de tipo funcional, fundado en la opción de simplificar el número de niveles para evitar crear una estructura excesivamente compleja. En concreto, la construcción del cuadro de clasificación se fundamenta en:

- La consolidación de cinco niveles, concretamente los referidos al fondo, la función, la serie documental, el expediente y la unidad documental.
- La codificación de cada nivel para generar una estructura normalizada. De esta manera, en cada una de las funciones básicas que se contemplen (cultura, urbanismo, etc.) las series documentales y los expedientes que las conforman, se encontrarán siempre en el mismo tipo de nivel.
- La correlación adecuada entre la estructura del Cuadro de Clasificación y las carpetas que se crean en el gestor documental.
- La inserción de metadatos que permitan identificar la relación de un expediente con la serie documental que le corresponde de manera automática.

La gestión del Cuadro de Clasificación es una competencia exclusiva del Archivo General que se concretará en:

- La administración, mantenimiento y actualización de la totalidad del cuadro de clasificación en tanto que instrumento integrador de los documentos y expedientes municipales.
- La posibilidad de integrar series documentales de nueva aparición por efecto de la aplicación de nuevas competencias municipales.
- La supresión de series documentales al cesar su aplicación por imperativo de carácter legal, o bien por la integración de distintas competencias en una nueva serie documental.
- La gestión del catálogo de tipologías documentales que prescribe el tipo de los documentos que integran un expediente.
- La integración del Cuadro de Clasificación con las Tablas de Evaluación Documental y con el cuadro de acceso a los documentos y su implementación automatizada a las oficinas municipales.

3.5.3 Descripción de los documentos

La clásica función de recuperación de la información contenida en los documentos y expedientes se concreta actualmente en dos instrumentos que trabajan en grado de complementariedad; de una parte, las normas internacionales emanadas del Consejo Internacional de Archivos, concretamente la ISAD (G) y la ISAAR (CPF) y de otra el modelo de metadatos desarrollado en las tres normas ISO 23081. En este caso, una propuesta específica y normalizada se deriva de la publicación de las Normas Técnicas del Esquema Nacional de Interoperabilidad (ENI) y la guía de Política de Gestión de Documentos y el Esquema de metadatos para la gestión del documento electrónico (e-EMGDE) el 2012.

En el caso del Ayuntamiento de Pamplona la base descriptiva se constituye a partir de la ISAD (G) y, más concretamente, en el modelo NEDA (Norma Española de Descripción Archivística) desarrollada por la Subdirección de archivos estatales que permite aplicar unos principios estandarizados de carácter internacional y también en la utilización del modelo de metadatos derivado del Esquema Nacional de Interoperabilidad.

Este modelo de metadatos se estructura en base a tres tipos de objetos (documentos, expedientes y firmas), cada uno de los cuales cuentan con un grupo de metadatos mínimos que deben adecuarse a la realidad y a los recursos municipales. El modelo de metadatos del ENI contiene 23 elementos que permiten una recuperación de la información a nivel administrativo, descriptivo y de preservación de amplio espectro.

3.5.4 Acceso y uso de los documentos

El acceso a la información contenida en los documentos es un derecho fundamental de una sociedad democrática y un elemento clave en la relación entre los ciudadanos y los poderes públicos. En el contexto español se percibe una falta de legislación específica

sobre acceso a la información en la medida que queda vinculada a las definiciones generales que recoge el artículo 105b) de la Constitución española, la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos, y a partir del 2 d'octubre de 2016 las leyes 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015 de Régimen jurídico del Sector Público y 39/2015 y el decreto de sistema español de archivos del 2011.

En todo caso, el acceso a la información se basa en la defensa de los derechos ciudadanos y en el fomento a la investigación, la docencia y la divulgación. Si bien los contenidos del acceso y uso de los documentos del Ayuntamiento se concretan en un protocolo específico, avanzamos unas directrices muy claras basadas en un modelo de acceso que concrete:

- La documentación accesible y los límites a la consulta.
- Las personas solicitantes y el grado de accesibilidad.
- El límite general de la finalización de un procedimiento.
- La información sobre documentos consultables y sobre limitaciones al acceso.
- La derogación de la reserva.
- Los aspectos procedimentales: solicitud de acceso, la denegación de acceso, los plazos de respuesta, la protección del derecho a la intimidad, el honor y la imagen, la protección de la propiedad intelectual e industrial y el fomento de la investigación.

En cuanto a la gestión interna del acceso, se plantea un modelo de roles y permisos que concrete los niveles de responsabilidad, las acciones que se pueden llevar a cabo (alta, modificación, eliminación de documentos) y las políticas de restricciones según el nivel de protección de los documentos. Más allá de la definición de diferentes niveles de responsabilidad, el modelo contempla la figura del administrador/es con amplia capacidad de actuación que se propone que recaigan en los responsables del Archivo General y el Servicio de informática.

3.5.5 Valoración, disposición, retención y calendario de conservación

A nivel general se acostumbra a definir la evaluación como la función destinada a determinar cuáles son los valores de los documentos según sus usos administrativos, fiscales y legales, tanto presentes como futuros, y sus valores testimoniales, informativos y de investigación. Su finalidad es garantizar que se conservarán para el futuro los documentos con valor permanente y que se procederá a la eliminación secuencial de los documentos con valores meramente coyunturales. En todos los casos, la evaluación debe situarse en el marco de un SGD y de una aparente contradicción: de una parte la necesidad ineludible de aplicar intensamente una técnica que reduce considerablemente los volúmenes documentales; de otra la reivindicación del interés de integrar otros fondos documentales –preferentemente de procedencia privada- en los archivos públicos. También cabe tomar en consideración que otorgar a los soportes digitales la virtud de

reducir el volumen de los documentos es un espejismo y, frecuentemente, una práctica insostenible económicamente.

La Norma ISO 15489-1 (9.2) destaca que las decisiones referentes al período de retención de los documentos en un sistema de gestión documental “se basan en la evaluación del marco normativo, de los requisitos de negocio y de la obligación de rendir cuentas y del riesgo”. En concreto, una adecuada gestión de la retención de documentos debe permitir responder a las necesidades de negocio presentes y futuras, cumplir los requisitos legales para garantizar que se ha documentado, se ha entendido y se ha implementado el marco normativo aplicable a la gestión documental para actividades del negocio específicas y responder a las necesidades presentes y futuras del grupo de interés y externos.

En este sentido, la misma norma 15489-1, explicita a grandes rasgos los documentos que es necesario retener de manera permanente:

- Los que proporcionan pruebas e información sobre las políticas y las acciones de la organización;
- Los que proporcionan pruebas e información referentes a la interacción entre la organización y la comunidad de clientes a quienes presta los servicios;
- Los que documentan los derechos y las obligaciones de las personas y las organizaciones;
- Los que contribuyen a la elaboración de la memoria de la organización con finalidades científicas, culturales o históricas;
- Los que contienen pruebas e información de las actividades que son importantes para los grupos de interés internos y externos.

La realidad práctica

En el Ayuntamiento de Pamplona, cualquier propuesta a realizar debe tomar en cuenta la existencia de una legislación foral que incide directamente sobre la política de valoración de los documentos. En concreto, nos referimos a la Ley Foral 12/2007, de archivos y documentos, y especialmente al Decreto Foral 75/2006, de 30 de octubre, que crea una Comisión de Evaluación Documental y un reglamento que regula su composición, organización y funcionamiento. Asimismo, mediante la Orden Foral 252/2007, se aprobó el modelo de ficha descriptiva de identificación de series documentales para su presentación a la Comisión de Evaluación Documental y también aprobó un modelo de acta de eliminación.

En atención al hecho que en el Ayuntamiento no se ha aplicado hasta el momento una política de evaluación de documentos para reducir el impresionante volumen de documentos que custodia el Archivo Municipal, más aquellos que aún permanecen en las oficinas municipales, parece razonable utilizar este cuerpo normativo de carácter foral para propiciar una acción decidida de evaluación y generar así el calendario de conservación para su aplicación global al Ayuntamiento.

En concreto se propone:

- La constitución formal por parte del Ayuntamiento de una Comisión Municipal de Evaluación Documental integrada por personal vinculado a los sectores de archivo y gestión documental, servicios jurídicos, servicios administrativos y el apoyo externo de un historiador contemporaneista. La creación de esta Comisión, así como la composición y designación de sus miembros debería formalizarse por acuerdo del Ayuntamiento. Esta Comisión Municipal generaría una política de valoración sistemática y exhaustiva, cuyos dictámenes podrían trasladarse a la Comisión creada por el gobierno de Navarra para su ratificación.
- La constitución de un manual que defina los valores y criterios para la valoración documental (administrativo, fiscal, jurídico-legal, informativo, testimonial e histórico) en el marco de la evaluación funcional.
- La generación de un calendario de conservación que señale para cada serie documental el período de retención y su concreción para la conservación temporal o permanente.
- La formalización de un acta de eliminación que permite cuantificar su alcance y características.
- La vinculación del calendario de conservación con las determinaciones del acceso a las series documentales.

3.5.6 Conservación y preservación a largo plazo

La preservación de los documentos electrónicos constituye un reto de gran relieve en la medida que cambia absolutamente los paradigmas de conservación de documentos en soporte papel y en un entorno legislativo y tecnológico extremadamente convulso. A la solidez visual y doctrinal de la conservación de documentos en papel se contraponen el carácter efímero y obsoleto de los soportes y las soluciones tecnológicas adoptadas en el último decenio.

En todo caso, en la adopción de una política de preservación a largo plazo de documentos electrónicos debe tomarse en cuenta el hecho que a diferencia de la conservación de documentos en papel que se realizaba en el ciclo final, en este caso inciden de manera directa una serie de factores que suponen un cambio relevante. En primer lugar, el hecho que la conservación/eliminación de los documentos electrónicos debe planificarse en el momento de su generación, la existencia de una abundante legislación y normativa internacional específica y también la necesidad de vincular esta preservación a las normas sobre firma electrónica, el acceso electrónico de los ciudadanos a los servicios públicos y la creciente normatividad sobre seguridad e interoperabilidad.

En este sentido es necesario evidenciar la profunda influencia del marco legal de la firma electrónica en los planes de preservación –básicamente la Ley 59/2003- en tanto que constituye un elemento ineludible en la definición de las funcionalidades de un repositorio o archivo electrónico y también el desarrollo de la resolución 19 de julio del 2011 por el que

se aprueba la Norma Técnica de Interoperabilidad de procedimientos de copiado auténtico y conversión entre documentos electrónicos que presenta cinco normas específicas sobre digitalización, documento electrónico, expediente electrónico, política de firma electrónica y de certificados de la Administración, y sobre los requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas.

Asimismo, cabe tener en cuenta las numerosas normas ISO que afectan las políticas de preservación como las normas 14721 (OAIS), 18492 (conservación a largo plazo de documentos electrónicos), 19005 (PDF/A), pero también las normas 15489 y 30300 sobre gestión de documentos y aquellas que se ocupan de la seguridad y el análisis de procesos.

Otro tema capital a considerar es el referido a la **sostenibilidad económica**. La percepción inicial que la conservación de los documentos electrónicos era fácil y económicamente poco costosa –producto de la fascinación inicial por las TIC y también por el hecho que se generaban pocos documentos en procesos de automatización- ha cambiado significativamente hasta el punto que actualmente existe una conciencia creciente que nos estamos refiriendo a un proceso de un coste tan notable que deviene fundamental en todo plan de gestión electrónica de documentos. En este sentido, proyectos europeos como ERPANET o LIFE, reafirman la certeza que no debería cometerse ningún plan de preservación sin un análisis exhaustivo de los costes derivados de su implantación y mantenimiento, sobre todo en el ámbito de la administración pública.

Por lo que se refiere a las **estrategias de preservación**, la continua evolución tecnológica caracteriza la obsolescencia del Hardware y Software, de manera que es necesario formular acciones planificadas que los expertos sintetizan en tres opciones: la conservación de la tecnología original, la emulación y la migración periódica. Dado que la conservación de la tecnología original deviene impracticable por su complejidad y coste (obligaría a la creación de verdaderos museos cibernéticos), y la emulación es muy costosa al tener que recrear las funcionalidades de la tecnología original, es en la migración periódica donde cabe situar el punto de atención.

Un elemento final a considerar es la reciente irrupción del concepto “*Cloud computing*” entendido como el almacenaje de información en la “*nube*” que implica la externalización de toda o parte de la información de una organización y de los datos que contienen. En una primera aproximación al tema sus ventajas y beneficios parecen evidentes (ahorro de costes, cesión de la gestión en manos de expertos) si bien también se plantean algunos inconvenientes que es necesario valorar adecuadamente. Entre éstos, el más relevante se refiere a la inseguridad jurídica que propicia una acción de este alcance. El experto francés Étienne Papin, en base a un análisis jurídico de la situación, tilda el cloud computing como una “*nebulosa jurídica*” y aporta sensatos argumentos a favor de una lectura más crítica de sus posibles beneficios. Por su parte el informe Inteco del mes de marzo de 2011 “*Riesgos y amenazas en el cloud computing*” sitúa la falta de confianza, principalmente en la gestión y control de los accesos (confidencialidad) y la gestión de datos (seguridad) como los problemas más notables.

Modelo propuesto

La plasmación en documentos de hechos y relaciones jurídicas responde a la necesidad de poder recuperar estos documentos en el futuro y usarlos como testimonios fiables de su contenido. Los documentos deben ser capaces de garantizar, durante un período largo de tiempo (ilimitado, en algunos casos), una serie de atributos clave:

- **Disponibilidad** de la información: La principal utilidad del documento es contener la información de tal manera que pueda ser recuperada en el futuro.
- **Inteligibilidad** de la información: La información ha de ser interpretable en el momento de la consulta, en términos fundamentalmente idénticos a como era presentada cuando el documento se generó.
- **Integridad** de la información contenida: El documento aspira no solo a contener la información, sino a ser testimonio de que la información no ha sido alterada, y que la información que se presenta representa la totalidad de lo que se capturó.
- **Autoría o Autenticidad**: El sistema de gestión documental aspira a ser capaz de acreditar que la documentación fue generada por la persona a quien se atribuye, en ejercicio de las facultades que le correspondían.

En plazos cortos de tiempo, estos objetivos se alcanzan mediante plataformas de gestión documental que apliquen técnicas estándar de seguridad de la información.

Cuando la organización desea garantizar estos objetivos a muy largo plazo, es necesario aplicar técnicas de preservación digital proactiva, para poder hacer frente a determinados riesgos propios de la documentación electrónica.

El Modelo de Preservación de Documentos Electrónicos definirá la estrategia a seguir en este sentido, proponiendo requisitos tecnológicos concretos y acciones proactivas de preservación. En todo caso, cabe tener en cuenta que la correcta aplicación, en las fases de tramitación, de los criterios de clasificación y descripción, así como el uso de formatos estándares, serán elementos fundamentales para permitir la aplicación de los criterios de preservación en los estadios posteriores.

3.6 Arquitectura tecnológica del Ayuntamiento de Pamplona

Por definición la gestión de documentos electrónicos requiere del soporte de una infraestructura tecnológica dotada de aplicaciones, bases de datos y sistemas operativos, en definitiva, sistemas de información. Es por ello que resulta indispensable contar con una adecuada definición, implantación y mantenimiento de la arquitectura tecnológica que dará apoyo a la gestión de documentos electrónicos y que deberá contar con los siguientes elementos:

1. **Módulo de gestión de la publicación de documentos a la Sede Electrónica** utilizado para publicar los documentos con validez jurídica, tal y como se establece

en la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos en los artículos: 10, 11 y 12 y, a partir del 2 de octubre de 2016, las leyes 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en sus artículos 45 y 131 y en la ley 40/2015 de Régimen Jurídico del Sector Público en el artículo 38 así como también podría utilizarse para publicar de forma segura la información de concursos y contratos de personal, obras y servicios y en el Tablón de Anuncios del Ayuntamiento.

2. **Portafirmas.** Plataforma que permite la visualización de documentos procedentes de los distintos procedimientos administrativos y distintas herramientas y la gestión de su firma electrónica. Permite la firma automatizada de documentos y expedientes con validez jurídica incluso de múltiples documentos a la vez con firma individualizada de cada uno.
3. **Plataforma de gestión de evidencias electrónicas.** Plataforma de gestión de las evidencias electrónicas que se van generando en los distintos procedimientos y que puedan ser aportados como prueba judicial del correcto desarrollo del procedimiento administrativo electrónico. Sustituirían por ejemplo a los vistos buenos en el entorno papel.
4. **Plataforma de digitalización segura de documentos.** Módulo que permite convertir el papel a documento electrónico con validez jurídica según la ley 11/2007 de acceso electrónico del ciudadano a los servicios públicos en su artículo 30 y, a partir del 2 de octubre de 2016, la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en su artículo 27.
5. **Módulo de impresión segura de documentos electrónicos.** Módulo que permite generar una copia en papel de un documento electrónico con validez jurídica, según la ley 11/2007 de acceso electrónico del ciudadano a los servicios públicos en su artículo 30 y, a partir del 2 de octubre de 2016, la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en su artículo 27.
6. **Plataforma de gestión de flujos de procedimientos administrativos (*workflow* o *BPM*).** Plataforma que permite el diseño y operación de procedimientos con el soporte de herramientas informáticas y expedientes y documentos electrónicos.
7. **Gestor documental.** Plataforma en la que se gestionan los documentos y los expedientes electrónicos tal y como se establece en la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos en sus artículos 10, 29 y 32 y, a partir del 2 de octubre de 2016, la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en sus artículos 26 y 70 y la ley 40/2014 de Régimen Jurídico del Sector Público en el artículo 38.
8. **Plataforma de custodia y preservación del expediente y documento electrónico.** Con el objetivo de garantizar a largo plazo la validez y acceso al documento y expediente electrónico es necesario disponer de herramientas de custodia tal y como establece la ley 11/2007 de acceso electrónico de los

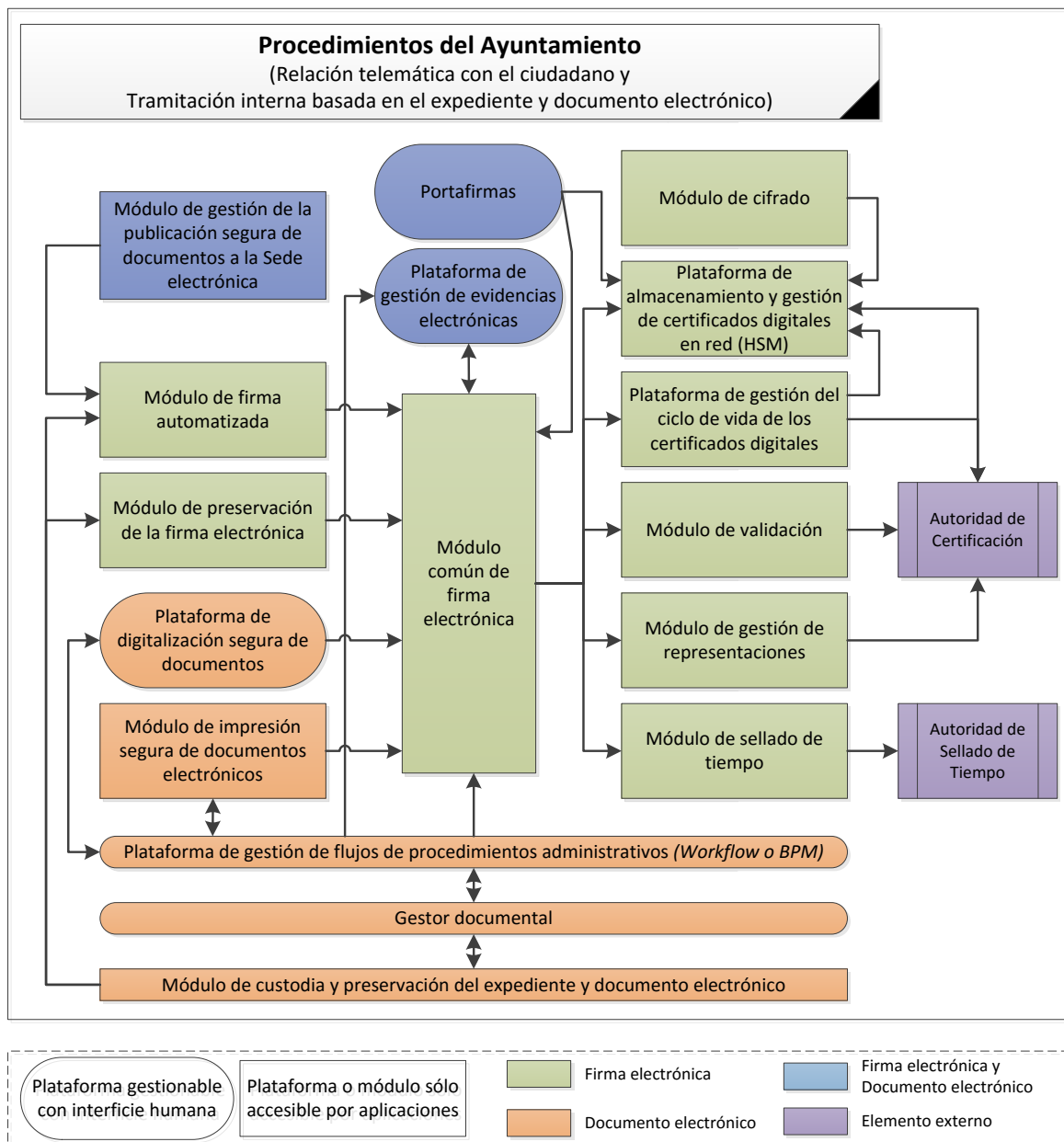
ciudadanos a los servicios públicos en su artículo 31 y, a partir del 2 de octubre de 2016, las leyes 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en su artículo 17 y 40/2014 de Régimen Jurídico del Sector Público en el artículo 46.

9. **Módulo común de firma electrónica.** Módulo que permite la generación de firmas electrónicas con diferentes formatos y a partir de documentos con diferentes formatos, tal y como se establece en la ley 11/2007 de acceso electrónico del ciudadano a los servicios públicos en sus artículos 13, 14, 15, 16, 17, 18, 19, 20, 21 y 22 y, a partir del 2 de octubre de 2016, la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en sus artículos 9, 10, 11 y 12, y en la ley 40/2015 de Régimen Jurídico del Sector Público en sus artículos 38, 40, 41, 42, 43 y 45 así como en la ley 59/2007 de firma electrónica.
10. **Módulo de firma automatizada.** Módulo que permite generar firmas electrónicas de forma automatizada, es decir, sin el control directo de ninguna persona. Resultará útil para el uso de certificados de sello electrónico en procesos de firma electrónica desatendida, pero también en la firma automatizada de personas físicas a partir del portafirmas.
11. **Módulo de preservación de la firma electrónica.** Módulo que permite completar una firma electrónica válida con sucesivos sellos de tiempo con algoritmos más robustos para garantizar la integridad de la firma electrónica y, en consecuencia, del documento firmado según establece la Norma Técnica de Interoperabilidad del documento electrónico en el punto 5.a del apartado II. Política de firma electrónica.
12. **Módulo de Cifrado.** Módulo que permite el cifrado y descifrado de documentos, mensajes, etc.
13. **Plataforma de almacenamiento y gestión de certificados digitales en red (HSM).** En inglés HSM, siglas de Hardware Security Module. Plataforma que permite gestionar de forma centralizada los certificados emitidos para el Ayuntamiento y que se guarda en un dispositivo criptográfico como dispositivo seguro de creación de firma.
14. **Plataforma de gestión del ciclo de vida de los certificados digitales.** Plataforma que permite la emisión y revocación de certificados digitales y el control eficiente de la información relacionada con los certificados disponibles en el Ayuntamiento.
15. **Módulo de sellado de tiempo.** Módulo que permite la generación de sellos de tiempo tal y como se establece en la ley 11/2007 de acceso electrónico del ciudadano a los servicios públicos y, a partir del 2 de octubre de 2016, las leyes 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de Régimen Jurídico del Sector Público.
16. **Módulo de validación.** Módulo que permite la validación de certificados digitales y de firmas electrónicas con distintos formatos, tal y como se establece la ley 11/2007 de acceso electrónico del ciudadano a los servicios públicos en sus artículos 13,

14, 15, 16, 17, 18, 19, 20, 21 y 22 y, a partir del 2 de octubre de 2016, la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en sus artículos 9, 10, 11 y 12, y en la ley 40/2015 de Régimen Jurídico del Sector Público en sus artículos 38, 40, 41, 42, 43 y 45, así como en la ley 59/2007 de firma electrónica.

17. **Módulo de gestión de representaciones.** Módulo que permite gestionar la capacidad de representación de personas con personas y de personas en representación de personas jurídicas, según establece la ley 11/2007 de acceso electrónico del ciudadano a los servicios públicos en su artículo 23 y, a partir del 2 de octubre de 2016, la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas en sus artículos 5 y 6.

La infraestructura tecnológica mencionada se expone a continuación a modo gráfico contemplando las interrelaciones que existen entre cada uno de sus elementos:



En este ámbito, el Ayuntamiento ha delegado en la Asociación Navarra de Informática Municipal S.A. (ANIMSA) el desarrollo, gestión y mantenimiento de sus sistemas de información en general y específicamente para la gestión de expedientes y documentos electrónicos. Estos sistemas de información están basados en las siguientes tecnologías y funcionalidades:

1. Formularios HTML a partir de los cuales se generan formularios PDF desarrollados con Adobe Live Cycle para el **inicio de la tramitación electrónica** por parte del ciudadano con posibilidad de adjuntar documentos electrónicos como complemento de la solicitud y, según el trámite, el requerimiento de firma electrónica del ciudadano.

2. Formulario HTML para las funcionalidades de **Registro electrónico** basadas en la identificación del ciudadano mediante certificado digital quien debe adjuntar el documento PDF generado en el paso anterior con los archivos adjuntos correspondientes y debidamente firmado por el ciudadano en formato electrónico. Como justificante de tramitación se genera un documento PDF que incluye los datos de tramitación y un resumen criptográfico de la documentación presentada (sobre el conjunto del PDF presentado y los documentos anexados), el cual es firmado automatizadamente con sello de órgano.
3. Buzón genérico de correo electrónico para la presentación electrónica de facturas mediante documento adjunto en formato *facturae*.
4. Las DLL de KSI para la **emisión y validación de firmas electrónicas** por parte del Ayuntamiento, tanto asistidas como automatizadas, y la validación de certificados digitales en el Registro electrónico para la identificación ciudadana electrónica. En ningún caso se completan las firmas con la información sobre su validación ni con sello de tiempo.
5. **Carpeta ciudadana** basada en una capa de visualización HTML cuya gestión de contenidos se realiza desde el gestor de expedientes.
6. Una herramienta única de **registro y gestión de expedientes** que contempla:
 - o una **única numeración de registro de entrada** independientemente del canal de presentación, telemático o presencial
 - o una **única numeración de registro de salida** independientemente de su origen, realizada por el funcionario o realizada a partir de un proceso automático como por ejemplo el proceso de notificación
 - o una **única numeración de expedientes** independientemente del soporte de su tramitación, en soporte papel o de documentos electrónicos, basada en una definición adhoc para cada procedimiento sin una nomenclatura homogénea preestablecida
 - o la **definición de flujos de proceso** con el soporte de datos en base de datos y de plantillas para la generación de documentos electrónicos pudiéndose generar tareas específicas para un expediente concreto fuera del flujo de procedimiento preestablecido
 - o la funcionalidad de **impresión segura** de documentos electrónicos incorporando al documento un Código Seguro de Verificación y una firma electrónica automatizada de sello de órgano
 - o la funcionalidad de **digitalización** que debido a que no incorpora firma electrónica, bien de funcionario habilitado en proceso asistido, bien de sello de órgano en proceso automatizado, obliga a mantener la documentación original en soporte papel.

- la funcionalidad de **notificación electrónica** a través de la carpeta ciudadana
 - la **conectividad con otros sistemas de información** del Ayuntamiento para la publicación de información y documentos en la carpeta ciudadana como por ejemplo volantes de empadronamiento o información sobre pago de tributos
 - la generación de un documento PDF con los datos del expediente y un índice de los documentos que lo conforman
 - una herramienta de **portafirmas** que permite establecer flujos de firma electrónica y la emisión de firmas de múltiples documentos con un único proceso de validación del certificado digital
 - un **gestor de representaciones** centralizado que en la actualidad no es consultado durante la tramitación telemática del ciudadano quien debe introducir datos de representante y representado para el inicio de un trámite sin comprobación automática alguna por parte del Ayuntamiento
7. La herramienta ALMADOC de **gestión de documentos electrónicos** en repositorio de ficheros o de base de datos accesibles a través del gestor de expedientes, del repositorio de documentos impresos de forma segura y de la carpeta ciudadana. El documento electrónico es accesible desde los distintos entornos sin replicarse en ningún caso. A nivel de metadatos se han implementado de forma parcial sobre el expediente durante su definición sobre el mismo gestor de expedientes y sobre el documento se recogen de forma automatizada con el soporte de una tabla de base de datos asociada al documento.
8. El Ayuntamiento cuenta con los servicios de **Camerfirma** para la emisión de certificados digitales. Esta Autoridad de Certificación proporciona además la plataforma de gestión del ciclo de vida de los certificados digitales y los servicios de sellado de tiempo y validación.

Los sistemas actuales permiten implementar de forma parcial los requerimientos definidos en relación con el ciclo de vida del documento electrónico. Es por ello que ANIMSA deberá trabajar en dotar a los sistemas de información actuales de las siguientes funcionalidades de aplicación específica para cada tipo de procedimiento en base a las directrices que emanan del presente Plan Director del Documento Electrónico. En el siguiente listado, las directrices se encuentran desarrolladas con todo detalle en el apartado sobre el Modelo tecnológico del documento y expediente electrónico de este Plan Director del Documento Electrónico.

1. Funcionalidades de **completitud de firmas electrónicas** con los datos de validación y sellado de tiempo con el objetivo de poder generar firmas tipo XAdES-XL y PAdES-XL independientemente si se trata de firmas emitidas por el Ayuntamiento como por el ciudadano.

2. El **control de los formatos de documentos** aceptados durante la tramitación electrónica tanto en la relación telemática con el ciudadano como durante la tramitación interna de procedimientos con el soporte del gestor de expedientes.
3. El **control de representación** a través de medios telemáticos bien sea a partir de los datos contenidos en el certificado digital o de la información contenida en el gestor de representaciones centralizado actual.
4. El **desarrollo de funcionalidades sobre el gestor expedientes**, según los instrumentos definidos en el presente Plan Director del Documento Electrónico, para:
 - El establecimiento de tipologías documentales a partir de las cuales generar las plantillas de los documentos que participan en cada procedimiento.
 - La implementación del Cuadro de Clasificación sobre los procesos soportados por la herramienta de gestión de expedientes.
 - La recogida automática o manual de los metadatos de expediente, documento y firma y, en consecuencia, sobre el gestor documental que lo soporta.
 - El control de los documentos mínimos que deben conformar un expediente.
 - La asignación de tiempos de preservación a cada expediente electrónico y los documentos y firmas que lo conformen según la Tabla de Evaluación Documental que les sea de aplicación. Con esta información el sistema debería realizar automáticamente propuestas de transferencia o eliminación de expedientes.
 - La digitalización segura de documentación papel mediante procedimientos de compulsión electrónica, asistidos por funcionarios habilitados que deban contrastar la imagen digitalizada contra el original y firmarla electrónicamente, o de digitalización certificada, realizados de forma automática mediante la firma automatizada de la imagen digitalizada con sello de órgano y con carácter previo al almacenamiento del documento.
 - El control automático de autorizaciones de representación según el gestor de representaciones centralizado tanto en la tramitación presencial como telemática.
5. El establecimiento de **procedimientos automáticos de foliado de expediente** sobre el gestor de expedientes que contemple la generación de un documento electrónico firmado electrónicamente con un sello de órgano del Ayuntamiento completado con sello de tiempo el cual incluya los datos del expediente en base de datos y un resumen criptográfico de los documentos que obligatoriamente deban conformar el expediente.

El procedimiento de foliado se realizará de forma automática al cierre del expediente por parte de los gestores del Ayuntamiento, momento en el que se

eliminarán automáticamente los documentos que no deban formar parte del expediente previa autorización de los responsables del procedimiento.

Como soporte al foliado de expedientes pueden considerarse documentos formato PDF/A con firma PAdES-A, XML con firma XAdES-LTV u otros formatos que garanticen su preservación a largo plazo. Deberán establecerse controles suficientes sobre este proceso que aseguren que se ejecutan con carácter previo a que cualquier firma electrónica contenida en el expediente pueda verse comprometida.

6. El desarrollo de **funcionalidades de gestión de documentos en fase semiactiva o de vigencia** sobre ALMADOC que permita, a partir del foliado del expediente, transmitir a un repositorio distinto de ALMADOC aquellos expedientes cuyos responsables decidan traspasar al Servicio de Archivo del Ayuntamiento (sólo con la información y documentación que debe formar parte del expediente resultado del mismo proceso de foliado).

A partir del momento de traspaso, el expediente y sus documentos sólo serán accesibles a partir de ALMADOC por parte del servicio de Archivo pudiendo el servicio responsable acceder a los metadatos de expediente, documentos y firmas mediante el gestor de expediente y, en caso de requerirlo, poder solicitar el acceso al Servicio de Archivo que le habilitará temporalmente a través del gestor de expedientes.

7. El desarrollo de **funcionalidades automáticas sobre ALMADOC de eliminación de expedientes electrónicos** en función de la Tabla de Evaluación Documental. Para ello ALMADOC propondrá al Servicio de Archivo qué expedientes pueden ser eliminados y tras su aprobación realizará los procesos de eliminación oportunos. Las mismas funcionalidades deberán ser implementadas sobre el gestor de expedientes ya que resultarán útiles en aquellos casos en que el expediente no haya sido traspasado al repositorio de ALMADOC para la fase semiactiva o de vigencia de gestión documental y la decisión deberá ser tomada por los mismos responsables del procedimiento.
8. El desarrollo de un **registro de evidencias electrónicas** que durante la tramitación electrónica de procedimientos y la realización de procesos de firma electrónica permita guardar registros informáticos o *log* incluyendo un resumen criptográfico del registro anterior y un sellado de tiempo de manera que garantice la integridad y el momento de realización del registro informático.

Adicionalmente, entre los sistemas actuales no existen funcionalidades para la fase de vigencia de expedientes, es decir, la conservación a largo plazo de documentos electrónicos mediante la migración de formatos y el resellado de tiempo de sus firmas electrónicas que garantice la legibilidad y validez de los documentos, respectivamente. En este sentido deberá identificarse una solución externa o desarrollarse internamente una solución tecnológica que permita al Servicio de Archivo del Ayuntamiento remitir desde ALMADOC aquellos expedientes en que pueda verse comprometidos los formatos de

documentos electrónicos y/o firmas electrónicas. Deberán establecerse automatismos para esta gestión que faciliten las tareas del Servicio de Archivo.

3.7 Aplicación del modelo documental a casos concretos

El modelo documental describe los instrumentos y herramientas sobre los que se cimienta la gestión de documentos en el Ayuntamiento. Sin embargo, a la hora de ponerlo en práctica en relación con expedientes y procedimientos concretos, será necesario analizar los documentos que participan en el procedimiento, su origen, su utilidad y uso esperado y la importancia que tienen para el Ayuntamiento.

En una estrategia de gestión basada en expediente electrónico, esta fase de análisis y diseño cobra una importancia fundamental. En el proceso de adaptación del procedimiento para su gestión con medios telemáticos se pueden simplificar y tipificar los trámites y documentos que se generan, y dicho análisis debería plasmarse en un documento de aplicación que describa como el modelo documental aplica al caso en concreto:

- Cómo y cuándo se genera el expediente
- Qué agentes participan en su creación, quién es el responsable y qué políticas de acceso le aplican
- Cómo se informarán los metadatos de expedientes de esta tipología, y qué metadatos pueden existir específicos de la serie documental correspondiente.
- Qué documentos lo conforman, como se generan, y en qué formatos.
- Qué documentos deben ir firmados, con qué tipo y formato de firma.

Este documento debería ser relativamente fácil de generar, fruto del análisis del procedimiento y de la aplicación de las reglas y políticas definidas en el modelo de gestión documental. Sin embargo, el hecho de plasmar estas decisiones en un documento de puesta en práctica facilita la fase de análisis funcional y diseño dentro del proceso de desarrollo de software, y permite a los usuarios finales y a los responsables de la gestión documental validar las decisiones que se hayan tomado.

4. Casos de uso

4.1 Casos de uso sobre tipologías de procedimiento

A continuación, se detallan algunos casos concretos de aplicación del modelo de gestión documental según distintas tipologías de procedimientos administrativos en los que interviene el uso de documentos electrónicos tal y como se prevé en este Plan y de cara a facilitar la comprensión de su aplicación. Para su desarrollo se ha tenido en cuenta el ciclo de vida de los documentos expuesto en el apartado anterior.

Exceptuando el último caso de uso, correspondiente al procedimiento donde se registre alguna información por medios telemáticos, para la implementación de un modelo de gestión basado en documentos electrónicos sobre un procedimiento debe considerarse siempre una primera fase análisis en el que se identifiquen los siguientes aspectos:

- El código del Cuadro de Clasificación al que pertenece el procedimiento.
- La Tabla de Evaluación Documental (TED) aplicable al procedimiento.
- Los documentos que conformarán el procedimiento y su formato durante la fase de tramitación. El formato a elegir dependerá no solo de la tecnología y de las herramientas de que dispone el Ayuntamiento sino también de la TED que sea de aplicación al procedimiento, para poder garantizar su preservación, si es el caso.
- El formato del documento de foliado del expediente y su contenido y orden, identificando los documentos que se eliminarán con carácter previo al procedimiento de foliado.
- Los flujos de firmas electrónicas que aplicarán a cada documento y el formato de las firmas.
- Los metadatos aplicables al expediente, a los documentos (incluido el de foliado) y a las firmas electrónicas y la forma de obtenerlas automáticamente o manual durante la tramitación del expediente o si se les puede asignar un valor por defecto.
- Los controles oportunos para identificar la necesidad de migración de formatos a lo largo de la vida del expediente.

Con este propósito se elaborarán unas fichas para cada tipo de procedimiento que se deberán cumplimentar en la fase de definición de cada procedimiento previa a su implementación sobre las herramientas tecnológicas que le darán soporte. En estas fichas, una por expediente y para cada documento y firma electrónica que forme parte de éste, se informará de todos los aspectos anteriormente especificados implementando las directrices de lo que en este Plan Director del Documento Electrónico se establece.

4.1.1 Procedimiento automatizado sin expediente

Esta tipología de procedimientos corresponde a aquellos servicios prestados a los ciudadanos sin intervención alguna de personal administrativo del Ayuntamiento. Ello es

posible gracias al procedimiento administrativo automatizado que permite la generación de documentos electrónicos de forma automática a partir de la información albergada en los sistemas de información del Ayuntamiento.

Los documentos generados de forma automatizada están dotados de validez jurídica a partir de la firma electrónica de los mismos mediante sello de órgano del Ayuntamiento la cual se completa con un sello de tiempo para garantizar su perdurabilidad en el documento obtenido por el ciudadano durante un período de tiempo razonable. Adicionalmente estos documentos se completan con un código seguro de verificación que permite su impresión de forma segura, es decir, sin que pierdan su valor al poder acceder a verificar su autenticidad con el documento electrónico original a partir de este código.

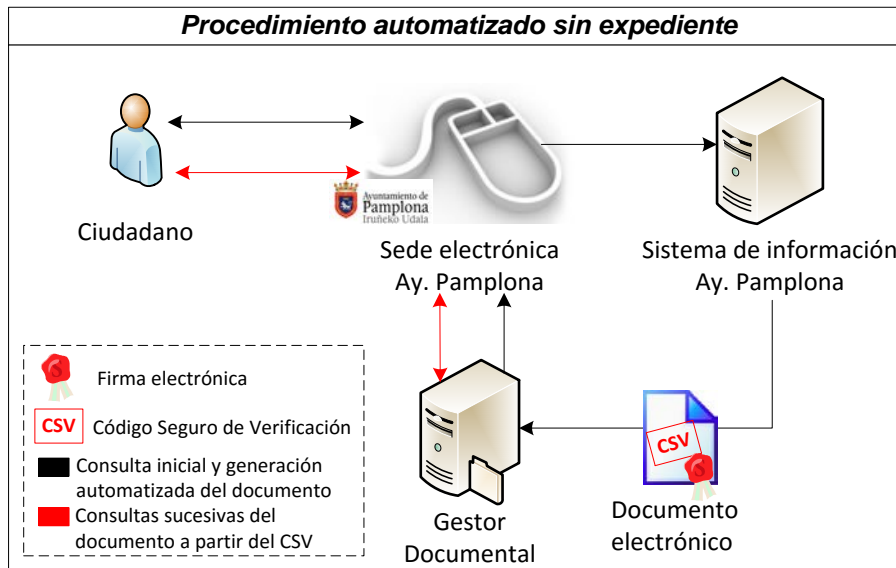
En este tipo de procedimientos el ciudadano obtiene documentos generados a partir de la información que consta en los sistemas de información del Ayuntamiento como por ejemplo la emisión de un certificado de pago de tributos o un volante de empadronamiento. Para ello se requerirá la integración entre sistemas de información, así como el establecimiento de medidas de control que garanticen la integridad, autenticidad y disponibilidad del proceso automatizado, así como a estrictas medidas de control que aseguren la adecuación del procedimiento a la normativa vigente en cada momento.

El procedimiento administrativo automatizado aplica sólo a aquellos de los cuáles se dispone en los sistemas de información de toda la información necesaria para la generación automática de la respuesta esperada por el ciudadano, así como están claramente reglados. Por lo tanto, quedan excluidos procedimientos en los que intervenga un acto de voluntad o la aplicación de criterios subjetivos por parte del Ayuntamiento, es decir, donde según la regulación que afecta al procedimiento el Ayuntamiento deba ejercer una potestad discrecional.

La documentación generada durante el procedimiento automatizado sin expediente, es decir, el documento generado para responder a la solicitud ciudadana, será almacenada en el gestor documental u otro repositorio accesible des de la sede electrónica sin generar expediente electrónico. Esta documentación se almacenará durante el tiempo en el que tendrá validez de manera que pueda ser accedida a partir de la introducción de su código seguro de verificación y comprobar su integridad y autenticidad. En su caso, se deberán aplicar procedimientos de resellado de tiempo sobre la firma electrónica del documento para garantizar su validez durante el tiempo en que deba ser válido. Adicionalmente, se deberán aplicar procedimientos automáticos de eliminación de documentos una vez éstos hayan dejado de tener validez.

Como ejemplo de este caso de uso estaría la obtención de un volante de empadronamiento o de un certificado de estar al corriente de pago de tributos.

A continuación, se incluye una representación gráfica simplificada de este caso de uso:



4.1.2 Procedimiento administrativo con inicio telemático, pero con expediente papel

Esta tipología de procedimientos corresponde a aquellos servicios iniciados por parte de los ciudadanos a través de medios telemáticos, pero que la tramitación interna del procedimiento por el personal del Ayuntamiento, exceptuando su resolución, se realiza en base a documentos en soporte papel dotados de validez mediante firma manuscrita.

En este tipo de procedimientos se ha resuelto el derecho del ciudadano, según la ley 11/2007 y, a partir del 2 de octubre de 2016, la ley 39/2015, a relacionarse con el Ayuntamiento a través de medios telemáticos, pero en cambio no se aprovechan las ventajas que genera el uso del documento electrónico.

Dado el hecho que la resolución del expediente realizada por el Ayuntamiento se realiza en soporte electrónico incluyendo Código Seguro de Verificación y firma electrónica de sello electrónico de órgano pueden darse las siguientes dos situaciones:

- Si el ciudadano prefiere la notificación en soporte papel esta deberá ser impresa y remitida en soporte papel a través del servicio tradicional de Correos.
- Si el ciudadano prefiere la notificación electrónica podrá utilizarse la funcionalidad ya existente en la carpeta ciudadana de la Sede electrónica del Ayuntamiento.

La evolución natural de la gestión de expedientes del Ayuntamiento será la de ir reduciendo el número de este tipo de procedimientos conforme se implanten todos los flujos de procedimientos sobre las herramientas de gestión de expedientes. En especial ello es debido a que se generan ineficiencias al tener que imprimir la documentación aportada en soporte electrónico por parte del ciudadano o al tener que digitalizar documentación generada en soporte papel por parte del Ayuntamiento para su entrega electrónica al ciudadano.

Adicionalmente, en este tipo de procedimientos deberán conservarse expedientes híbridos en donde la documentación aportada por el ciudadano será original en su formato electrónico y la documentación generada por el Ayuntamiento será original en su formato papel.

Si bien es cierto el punto anterior, también es cierto que determinados procedimientos que se ejecuten pocas veces en un ejercicio, pueda ser esta la mejor opción, puesto que los costes derivados de la digitalización de todo el procedimiento pueden ser muy altos comparados con el beneficio que pueda aportar.

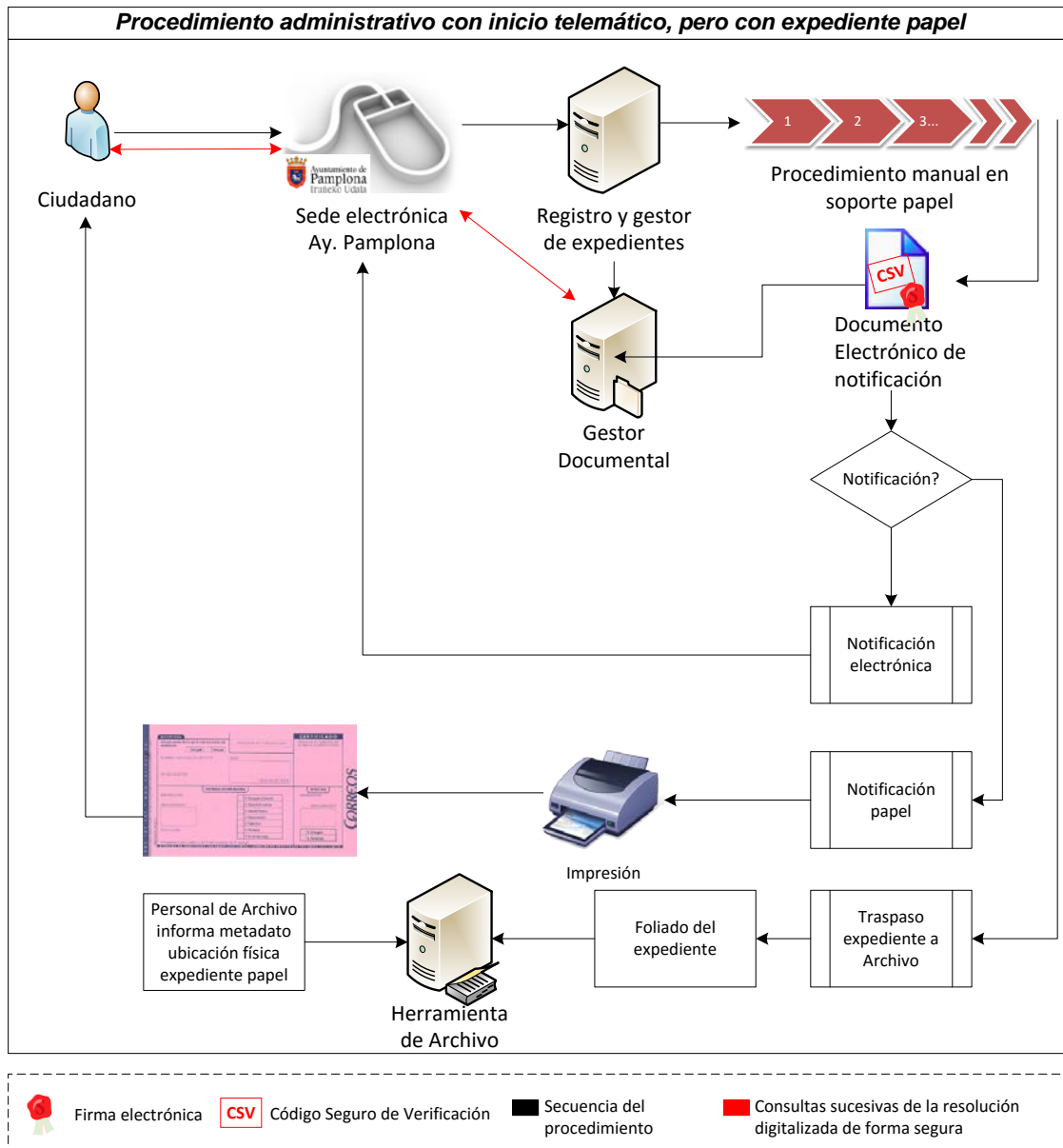
La documentación recibida y generada durante la tramitación electrónica deberá ser almacenada en el gestor documental, concretamente el documento de solicitud firmado por el ciudadano y la documentación que anexe durante la tramitación y el justificante de tramitación electrónica emitido por el Ayuntamiento. Esta documentación será accesible a través del gestor de expedientes, el cual le otorgará la numeración de expediente, hasta que el servicio responsable del Ayuntamiento decida su traspaso a la herramienta de archivo. Este traspaso deberá realizarse siempre con carácter previo a que pueda comprometerse la firma electrónica del ciudadano la cual será completada con un sello de tiempo en el momento de su recepción y validación.

Para el traspaso se generará el foliado del expediente el cual incluirá la información del expediente y un resumen criptográfico de los documentos electrónicos que lo componen firmado con sello de órgano del Ayuntamiento y completado con sello de tiempo. En función de los requerimientos de preservación del expediente, la herramienta de Archivo aplicará técnicas de resellado de la firma electrónica del documento de foliado y, en caso de resultar necesario, migraciones de formatos de los documentos relacionados.

La existencia de documentación en soporte papel que formará parte del expediente obligará a que el personal de archivo indique en el gestor documental la ubicación física del expediente papel una vez recibida la transferencia del mismo. Para ello se informará el metadato relacionado correspondiente el cual hasta su traspaso a archivo estará sin informar o indicará "archivo departamental". Cabe mencionar que en estos casos, el expediente se considerará híbrido.

Como ejemplo de este caso de uso estaría cualquier solicitud recibida a través de la Sede electrónica haciendo uso de la instancia general y que no disponga de un procedimiento establecido en el gestor de expedientes.

A continuación, se incluye una representación gráfica simplificada de este caso de uso:



4.1.3 Procedimiento administrativo totalmente digitalizado

Esta tipología de procedimientos corresponde a aquellos servicios prestados a los ciudadanos a través de medios telemáticos o procedimientos internos cuya tramitación por parte del personal del Ayuntamiento hasta su resolución se realiza en base a documentos electrónicos dotados de validez mediante firma electrónica y con el soporte del flujo de procedimiento correspondiente sobre las herramientas informáticas de gestión de expedientes del Ayuntamiento.

En este tipo de procedimientos se ha resuelto el derecho del ciudadano, según la ley 11/2007 y, a partir del 2 de octubre de 2016, la ley 39/2015, a relacionarse con el Ayuntamiento a través de medios telemáticos y además se aprovecha las ventajas que genera el uso del documento electrónico. Para la resolución del procedimiento el ciudadano

podrá optar por la notificación papel hecho que forzará al Ayuntamiento a generar una copia auténtica del documento electrónico de resolución mediante un documento electrónico con el mismo contenido, una firma electrónica con el sello de órgano del Ayuntamiento y un código seguro de verificación que permita su impresión segura.

La evolución natural de la gestión de expedientes del Ayuntamiento será la de ir ampliando el número de este tipo de procedimientos hasta su totalidad, exceptuando los procedimientos automatizados sin expediente.

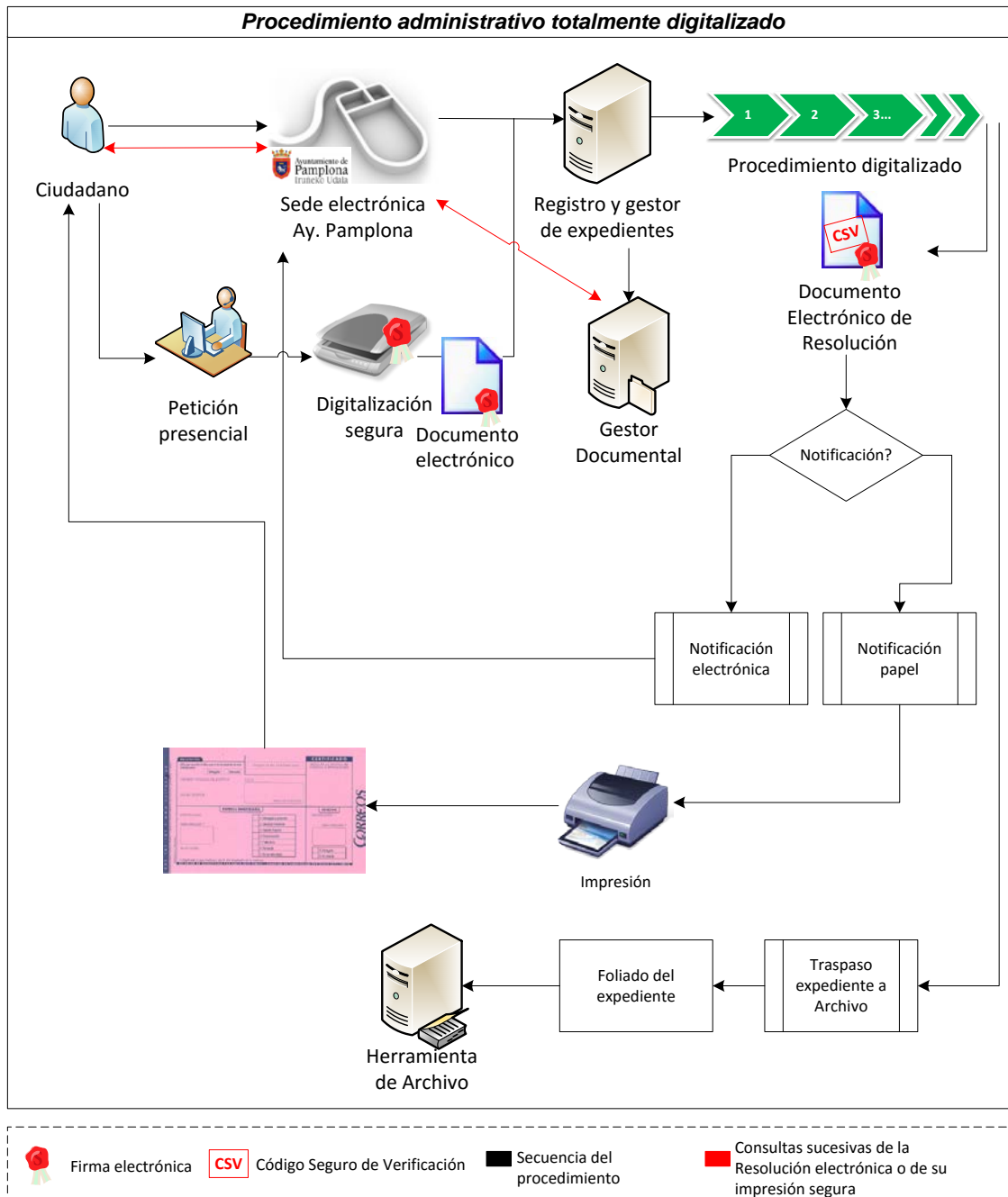
En este tipo de procedimientos sólo existirán documentos electrónicos habida cuenta que la documentación generada por el Ayuntamiento lo es en este formato y, en caso de que el ciudadano opte por la relación presencial con el Ayuntamiento, la documentación que aporte en soporte papel será destruida tras su digitalización de forma segura.

La documentación generada durante la tramitación electrónica deberá ser almacenada en el gestor documental, concretamente el documento de solicitud firmado por el ciudadano y la documentación que anexe durante la tramitación, así como la documentación generada internamente durante la resolución de la solicitud. Esta documentación será accesible a través del gestor de expedientes hasta que sus responsables decidan su traspaso a la herramienta de archivo siempre con carácter previo a que pueda comprometerse las firmas electrónicas existentes, tanto las del ciudadano como las del personal del ayuntamiento, las cuales serán completadas con un sello de tiempo en el momento de su recepción o emisión, respectivamente, y validación.

Para el traspaso se generará el foliado del expediente el cual incluirá la información del expediente y un resumen criptográfico de los documentos que lo componen firmado con sello de órgano del Ayuntamiento y completado con sello de tiempo. En función de los requerimientos de preservación del expediente, la herramienta de Archivo aplicará técnicas de resellado de la firma electrónica del documento de foliado y, en caso de resultar necesario, migraciones de formatos de documentos.

Como ejemplo de este caso de uso estaría el procedimiento de validación de facturas en base a documentos y expedientes electrónicos o una solicitud de licencia de apertura (actividad inocua) o una licencia de primera utilización.

A continuación, se incluye una representación gráfica simplificada de este caso de uso:



4.1.4 Procedimiento administrativo con inicio presencial, pero con expediente electrónico

Igual que en el caso anterior, esta tipología de procedimientos corresponde a aquellos servicios prestados a los ciudadanos a través de la aportación presencial de documentos cuya tramitación por parte del personal del Ayuntamiento hasta su resolución se realiza en base a documentos electrónicos dotados de validez mediante firma electrónica y con el soporte del flujo de procedimiento correspondiente sobre las herramientas informáticas de gestión de expedientes del Ayuntamiento.

Con carácter general el ciudadano sigue manteniendo la posibilidad de relacionarse con el Ayuntamiento mediante una relación presencial y, por consiguiente, haciendo uso de documentación en soporte papel.

En este tipo de procedimientos el funcionario del Ayuntamiento que atiende presencialmente al ciudadano introduce en el sistema de registro general y de gestión de expedientes toda la información relativa a la solicitud ciudadana y, en su caso, digitaliza de forma segura la documentación aportada por el ciudadano. A partir de aquí la tramitación interna se realiza según el flujo de procedimiento establecido en el gestor de expedientes electrónicos.

El ciudadano podrá escoger el canal preferente de notificación, es decir, papel o electrónica y se requerirá la impresión segura de la resolución o el uso de la plataforma de notificación electrónica con el documento electrónico de resolución, respectivamente.

Se presupone que al final del proceso de adopción de la Administración electrónica todos los procedimientos, exceptuando los procedimientos automatizados sin expediente recaerán sobre este modelo de procedimiento permitiendo a la vez la posibilidad de su inicio telemático por parte del ciudadano.

En este tipo de procedimientos sólo existirán documentos electrónicos habida cuenta que la documentación generada por el Ayuntamiento lo es en este formato y, en caso de que el ciudadano escoja la relación presencial con el Ayuntamiento la documentación que aporte en soporte papel será destruida tras su digitalización de forma segura.

La documentación generada durante la tramitación electrónica deberá ser almacenada en el gestor documental, concretamente la documentación aportada por el ciudadano digitalizada de forma segura, así como la documentación generada internamente durante la resolución de la solicitud. Esta documentación será accesible a través del gestor de expedientes hasta que el servicio responsable del Ayuntamiento decida su traspaso a la herramienta de archivo siempre con carácter previo a que pueda comprometerse las firmas electrónicas existentes, tanto las del ciudadano como las del personal del ayuntamiento, las cuales serán completadas con un sello de tiempo en el momento de su recepción o emisión, respectivamente, y validación.

Para el traspaso se generará el foliado del expediente el cual incluirá la información del expediente y un resumen criptográfico de los documentos que lo componen firmado con sello de órgano del Ayuntamiento y completado con sello de tiempo. En función de los requerimientos de preservación del expediente, la herramienta de Archivo aplicará técnicas de resellado de la firma electrónica del documento de foliado y, en caso de resultar necesario, migraciones de formatos de documentos.

A nivel de representación gráfica simplificada sería de aplicación el gráfico incluido en el apartado anterior. Como ejemplos nos referimos también al apartado anterior.

4.1.5 Procedimiento donde se registre alguna información por medios telemáticos

Esta tipología de procedimientos corresponde a aquellos servicios prestados a los ciudadanos a través de medios telemáticos que permiten la introducción de información directamente sobre los sistemas de información del Ayuntamiento sin que ello genere un expediente administrativo.

Lo más habitual es que el ciudadano a través de la tramitación telemática o la carpeta ciudadana pueda introducir información como por ejemplo el correo electrónico a efectos de notificación o un número de cuenta bancaria a efectos de pago de tributos que en caso de considerarse necesario realizará el correspondiente justificante de registro de entrada. Adicionalmente, a través de la carpeta ciudadana el ciudadano podrá consultar la información con carácter previo a su modificación.

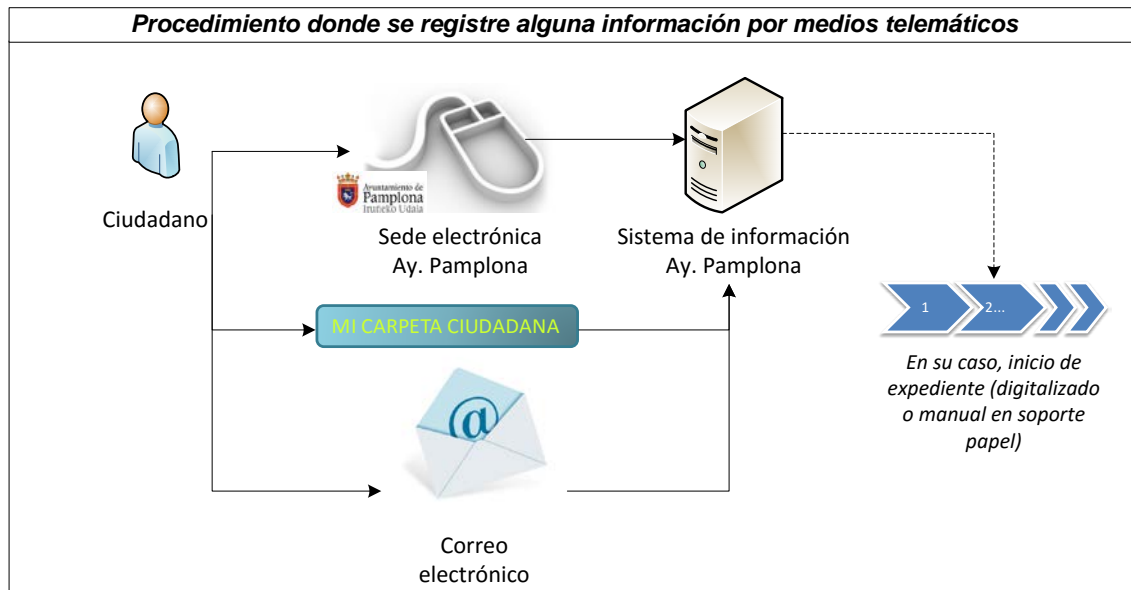
Por otro lado, también se contempla la posibilidad de que el ciudadano remita un correo electrónico con la información que permita al personal del Ayuntamiento realizar los cambios oportunos en sus sistemas de información.

Este tipo de procedimiento se reserva a aquella información de carácter accesoria a la actividad administrativa reglada del Ayuntamiento y/o que pueda ser verificada con posterioridad aplicando, en su caso, el régimen sancionador correspondiente. Por lo tanto, en este tipo de procedimientos no será guardará documentación alguna en el gestor de documentos sino sólo modificaciones e introducción de datos en las bases de datos de los sistemas del Ayuntamiento.

Como ejemplo de este caso de uso estaría la comunicación a través de la carpeta ciudadana del correo electrónico a efectos de notificación electrónica o de la cuenta bancaria para el pago de tributos.

No obstante, lo anterior, en ocasiones, en este tipo de procedimiento es posible que el personal del ayuntamiento dé inicio a un expediente como puede ser el caso del defensor del pueblo cuyo inicio de expediente se realiza a partir de la recepción de un correo electrónico. La gestión de expedientes se realizaría con el soporte de documentos papel y/o electrónicos según sea su nivel de implementación sobre los sistemas de gestión de expedientes y documental del Ayuntamiento.

A continuación, se incluye una representación gráfica simplificada de este caso de uso:



4.2 Ejemplo de arquitectura tecnológica de gestión documental

Como ejemplo de arquitectura tecnológica de gestión documental nos referimos al apartado 3.5 de este Plan Director del Documento Electrónico. En este apartado se define la arquitectura tecnológica del Ayuntamiento de apoyo a la gestión de documentos electrónicos partiendo de la definición de los elementos básicos que deben conformarla y sus interrelaciones.

4.3 Ejemplo de un proceso de digitalización masivo: interno y externo.

La digitalización es el proceso por el cual se obtienen imágenes digitales de documentos en soporte papel tal y como se describe en detalle en el apartado de Modelo de digitalización del presente Plan Director del Documento Electrónico.

En los procedimientos llevados a cabo por el Ayuntamiento es posible que se requiera la realización de procesos de digitalización masivos. Con estos procesos se realiza la digitalización de un gran volumen de documentación la cual es asociada, mediante la asignación automática de metadatos, al registro informático correspondiente como por ejemplo un registro de entrada o un expediente.

4.3.1 Ejemplo de un proceso de digitalización masiva: interno.

El Ayuntamiento dispone de un proceso de digitalización masivo basado en la digitalización de documentos de acuse de recibo de notificación. El proceso se basa en los siguientes pasos:

- agrupar los acuses de recibo por el resultado de la notificación (aceptada, rechazada, etc.)
- seleccionar la opción del gestor de expedientes electrónicos correspondiente al resultado de la notificación
- digitalizar los documentos con el sistema de alimentación automática del elemento hardware de digitalización
- durante el proceso de digitalización, automáticamente, se interpreta el código de barras que lleva incluido cada documento y lo vincula con el expediente correspondiente desde el que puede ser accedido, aunque sea almacenado en el gestor documental ALMADOC

Actualmente, durante el proceso expuesto se completan de forma automática ciertos metadatos que caracterizan el documento como son el formato, el tamaño o el expediente al que pertenecen. No obstante, no se ha aplicado el vocabulario de metadatos completo del Ayuntamiento.

En el momento de la implementación del vocabulario de metadatos sobre los procedimientos de digitalización, el Ayuntamiento deberá considerar la máxima automatización en el proceso de completar los metadatos del documento electrónico resultante de la digitalización y, en su caso, forzar al usuario final a rellenar el resto.

4.3.2 Ejemplo de un proceso de digitalización masiva: externo.

El Ayuntamiento de Pamplona dispone de un servicio externalizado de digitalización de la documentación que se presenta por Registro de Entradas. El procedimiento seguido es el siguiente:

- En la aplicación de registro de entradas se genera la entrada, se indica el número de páginas a digitalizar y se genera un justificante que incluye un código de barras. Este justificante se ubica como portada de la documentación papel aportada.
- Al final del día se genera un albarán de entrega a la empresa que realizará la digitalización y en el que figuran la relación de registros de entradas con documentos a digitalizar, su código de barras y el número de páginas a digitalizar.
- La empresa de digitalización recibe la documentación a través de un canal seguro y de forma automatizada digitaliza la documentación en unidades documentales según la portada de cada documento. A partir de esta portada, el sistema comprueba automáticamente que el número de páginas digitalizadas coincide con las informadas en el justificante y, en caso contrario, genera el error correspondiente.
- En el proceso de digitalización se asigna automáticamente y manual el conjunto de metadatos establecidos, entre ellos la información relativa al número de registro de entrada, el número de páginas del documento o su formato. Adicionalmente se firma

automatizadamente cada documento con un sello electrónico de la empresa para dotarlo de validez jurídica y poder destruir la documentación original tras la incorporación de la documentación en los sistemas del Ayuntamiento.

- El documento digitalizado resultante es un PDF que se incluye en un XML que contiene también los metadatos del fichero. Este fichero se facilita al Ayuntamiento mediante servicios web y a partir de sus metadatos se almacena en el Registro de entradas. Previamente se realiza una verificación automática de su contenido e integridad y se elimina la firma electrónica de la empresa externa y se firma con el sello de órgano del Ayuntamiento.
- Se han establecido procedimientos periódicos para la auditoría del proceso que aseguren su integridad, autenticidad y trazabilidad.

4.4 Ejemplo de un sistema de preservación de documentos.

La validez, disponibilidad y accesibilidad de un documento electrónico a largo plazo depende de dos factores clave:

1. La validez de la firma electrónica sujeta a la caducidad del certificado digital con el que se firmó o se completó con un sello de tiempo.
2. La obsolescencia tecnológica de los formatos documentales.

Tal y como se expone con mayor detalle en el apartado de Modelo de Preservación de este Plan Director del Documento Electrónico, para resolver esta complejidad se requiere de herramientas tecnológicas de preservación y custodia documental que, durante el tiempo que el documento deba ser válido según la Tabla de Evaluación Documental asignada, realicen tras recibir el documento desde la herramienta de gestión documental:

1. El resellado de tiempo de sus firmas electrónicas.
2. La migración de su formato hacia un nuevo formato con garantías suficientes de apertura prolongada o, en su defecto, la aplicación de controles compensatorios que faciliten la apertura del documento en el formato actual.

Por lo tanto, la preservación que desee asignarse a cada documento electrónico es un aspecto clave a considerar en la fase de definición del procedimiento con el que se generará y/o gestionará con respecto a:

1. El tipo de firma electrónica a utilizar, es decir, el completado de la misma con información de validación de la firma o sellado de tiempo.
2. El formato documental a utilizar.

Adicionalmente, el sistema de preservación de documentos deberá contar con funcionalidades de ingreso, consulta y administración de la plataforma además de las ya expuestas de preservación.

A modo de ejemplo puede considerarse la herramienta iARXIU del Consorcio AOC de la Generalitat de Catalunya.

4.5 Ejemplo de un sistema de preservación de la firma de documentos.

Es posible que la misma herramienta de gestión documental requiera de elementos de preservación de firma electrónica debido a que el expediente y sus documentos por estar en fase de tramitación o vigencia aún no han sido traspasados al sistema de preservación de documentos o fase histórica.

En este sentido puede considerarse lo siguiente:

- Completar la firma electrónica de un ciudadano con un sello de tiempo de manera que su firma sea válida hasta la caducidad del certificado digital que generó el sello de tiempo y no hasta que caduque el certificado digital del ciudadano (que en el peor de los casos podría ser al día siguiente).
- Automatismos sobre la herramienta de gestión documental que identifiquen la proximidad de caducidad de una firma electrónica o de su sello de tiempo y generen una propuesta para su resellado utilizando servicios específicos de firma electrónica.
- Automatismos que permitan identificar la longitud de las claves criptográficas del certificado electrónico con el que se generó la última firma o sellado de tiempo de un documento electrónico y generen una propuesta de resellado para todas aquellas que podrían verse comprometidas utilizando un certificado digital con claves criptográficas de mayor longitud.

El Ayuntamiento utiliza la DLL de KSI la cual con desarrollos a medida podría cubrir lo que se ha expuesto. En el mercado también existen otras soluciones como las que proveen los proveedores HP o SafeLayer.

5. Modelo organizativo

5.1 Necesidad de un modelo organizativo

Con la introducción del documento electrónico y, sobre todo, los mecanismos de tramitación automatizada de los procedimientos, se producen importantes cambios en la manera de trabajar de una organización. Estos cambios afectan no solamente a las herramientas tecnológicas en las que se apoyan los miembros de la organización, sino también a la forma en que las personas desempeñan tareas que podrían parecer básicas.

De esta manera, actividades tan cotidianas como la emisión de certificados, la compulsión de copias o la clasificación y archivo de documentos cambian radicalmente y requieren de un nuevo enfoque.

Este cambio de enfoque requiere de una adaptación de la organización a varios niveles:

1. **Gestión del cambio:** Por una parte, en lo que se refiere a la manera de trabajar de las personas, es necesaria una política definida de gestión del cambio, que les ayude a asumir como propio el nuevo modelo de organización y a identificar:
 - Qué nuevas herramientas están a su disposición
 - De qué manera cambian sus procedimientos de trabajo
 - Qué nuevas tareas deben desempeñar, y cuáles dejan de corresponderles

Este proceso de gestión del cambio debe conducirse de una manera que haga que las personas se sientan cómodas en el nuevo contexto, ofreciendo soluciones para aclarar las dudas que puedan tener sobre el proceso de cambio y trasladando el mensaje de que la organización tiene una visión clara de cuál es el modelo de trabajo que se pretende y del lugar que cada persona ocupará en él.

2. **Modelación y simplificación de procedimientos:** Por otra parte, en lo que se refiere a la definición de procedimientos y metodologías de trabajo, resulta imprescindible un enfoque más sistemático en la definición *a priori* de los procesos de toma de decisiones y de generación y gestión de la información.

Todas las ventajas que ofrecen la automatización de procedimientos y la incorporación de documentos electrónicos parten de la capacidad de la organización para establecer criterios claros que permitan automatizar la toma de decisiones.

Para poder aprovechar estas ventajas en un procedimiento electrónico, es necesario hacer un análisis detallado de los casos que se pueden dar, los comportamientos que se esperan del sistema y las acciones que deben realizar las personas en cada escenario que se pueda prever.

La modelación del procedimiento va siempre ligada con el concepto de simplificación y reingeniería. Esta es la idea de que, aprovechando el impulso de análisis autocrítico que comporta la modelación, se busquen oportunidades para:

- Eliminar pasos superfluos
- Simplificar acciones
- Unificar actuaciones para reducir la complejidad del proceso
- Introducir elementos de interoperabilidad para simplificar la interacción con otras organizaciones.

A continuación, realizaremos una serie de propuestas relacionadas con la simplificación y modelación de procedimientos.

3. **Definición de la estructura de los expedientes:** Cuando trabajamos con documentos en papel, los procedimientos pueden ser difusos porque los mecanismos para generar o recuperar un documento o para componer un expediente son adaptados *ad hoc* por las personas que participan en ellos. Si la organización quiere confiar estos procesos a sistemas automáticos, es necesario poder establecer criterios claros para decidir cuestiones como

- Qué documentos deben formar un expediente
- Cómo y cuándo se deben generar
- Cómo se deben etiquetar y describir
- Dónde deben custodiarse y por cuánto tiempo
- Qué personas pueden acceder a ellos.

Lo que se requiere, por tanto, es complementar el proceso de modelación y simplificación de procedimientos con un análisis detallado de los componentes de gestión documental que condicionan el expediente, como se desarrolla en el apartado 5.4.

4. **Responsabilidades de los agentes que impulsan el cambio:** La gestión del cambio no sólo es relevante en relación con los trabajadores que deben adaptarse a las nuevas metodologías. Es crucial también gestionar la manera como los líderes de la organización se involucran en el proceso de cambio, y es fundamental establecer roles claros en el proceso de modernización. A continuación, haremos una propuesta sobre como atribuir estas responsabilidades.

5.2 Gestión del cambio

El proceso de implantación del documento electrónico en el Ayuntamiento supone el paso de una administración basada en el documento papel y la relación presencial con la ciudadanía a una administración basada en el documento electrónico con validez jurídica, la gestión digitalizada de procedimientos y la relación telemática con la ciudadanía.

En este apartado se indican las principales actuaciones que el Ayuntamiento puede efectuar para:

1. Facilitar la difusión de los proyectos de Modernización. Es necesario que los destinatarios de los proyectos de modernización sean concededores de los mismos y puedan utilizarlos sin incidencias, evitando así que el desconocimiento o el bajo grado de uso limiten el retorno de la inversión.
2. Formar al personal que participe en los proyectos de modernización en sus nuevas atribuciones que faciliten asumir internamente la carga de los proyectos que deben acometerse, así como que estos se realicen exitosamente y puedan mantenerse y evolucionar convenientemente en el tiempo.

5.2.1 Acciones de Difusión

Se considera básico actuar en tres ámbitos:

- Disponer de un repositorio web donde encontrar toda la información sobre los conceptos de documento electrónico y e-Administración y como se prevé su implantación en el Ayuntamiento
- Realizar un conjunto de sesiones de información, ya sean presenciales o a través de técnicas de eLearning, para comunicar a los empleados del Ayuntamiento el despliegue del modelo de Gestión Documental y cómo impacta en el enfoque que el Ayuntamiento da a la gestión y en particular a la e-Administración.
- Realizar un conjunto de actuaciones de difusión entre la ciudadanía sobre la puesta en marcha de nuevos servicios telemáticos aprovechando los canales de comunicación ya existentes en el Ayuntamiento.

5.2.2 Acciones de Formación

Se considera básico actuar a dos niveles

1. **Formación específica vertical.** Orientada a dar los conocimientos específicos a ciertos colectivos para que puedan participar activamente en el proceso de adopción del documento electrónico. Esta formación estaría dirigida a personal del Ayuntamiento de los siguientes ámbitos:
 - Tecnológico
 - Jurídico
 - Organizativo-procedimental,
 - Gestión documental

Se recomienda disponer además de esta formación en formato eLearning para facilitar la difusión de estos conocimientos clave entre las distintas personas involucradas en proyectos de e-Administración.

2. **Formación vinculada a la puesta en marcha de los nuevos servicios.** En este ámbito estarían el conjunto de formaciones específicas cada vez que se ponga en marcha un nuevo servicio. Así, por ejemplo, estarían en este ámbito la formación a al personal de registro para que conozcan cómo impacta en el funcionamiento del registro la implantación del modelo de gestión documental, o la formación del personal que va a gestionar de forma digital un determinado proceso que se ha procedido a su digitalización.

5.3 Metodología de simplificación y reingeniería de procesos

Un factor importante a la hora de aprovechar las oportunidades de ahorro y eficiencia que ofrece la implantación de la Administración Electrónica es que la organización sea capaz de analizar con criterio crítico sus propios procedimientos de trabajo, mejorándolos, racionalizándolos y simplificándolos para explotar al máximo las posibilidades que ofrece la gestión electrónica de procedimientos, la interoperabilidad, la tramitación automatizada y la relación telemática.

Para poder abordar con éxito la reingeniería de procesos es fundamental, por tanto:

- Atribuir formalmente, dentro de la organización, un rol de responsable de organización, procesos o calidad. Es posible que, por la particular relación que existe entre el Ayuntamiento y ANIMSA, un modelo adecuado sea el de atribuir estas competencias a la propia empresa de servicios, pero sería importante que esta atribución se formalizaría de alguna manera, ya que existe una diferencia en las competencias y responsabilidades entre:
 - Responsables tecnológicos, cuya prioridad es disponer de herramientas que sirvan a los fines de la organización y proporcionar soluciones para la gestión de la información, y
 - Responsables organizativos, cuya prioridad es garantizar que las metodologías de trabajo y las herramientas son las adecuadas para que las personas de la organización puedan cumplir con su cometido, y las que permiten optimizar esfuerzos y minimizar los recursos invertidos en la realización de las tareas troncales de la organización.
- Disponer de una metodología de análisis de procedimientos, que garantice que en el proceso de análisis crítico y modelación de un procedimiento de trabajo:
 - Se involucra a todas las personas relevantes para el análisis de este procedimiento en concreto.

- Se tienen en cuenta los recursos y herramientas de que ya dispone la organización, humanos, materiales, tecnológicos y metodológicos.
- Se aplican de manera sistemática una serie de criterios de optimización y sistematización.
- Se plasman las decisiones tomadas en un soporte que permita no sólo la implementación inmediata sino su revisión futura.

El Ayuntamiento deberá disponer, por tanto, de una metodología que identifique:

- Las fases del proceso de análisis, mejora, simplificación y reingeniería del procedimiento.
- La fase de diseño del nuevo procedimiento.
- La fase de implantación del nuevo procedimiento.
- Los documentos resultantes y las responsabilidades de todo el proceso.

Los objetivos a perseguir por parte de esta metodología deberán ser:

- Disminuir las cargas administrativas a ciudadanos y empresas.
- Disminuir las cargas de gestión para el mismo órgano administrativo.
- Maximizar los puntos fuertes de los procesos actuales y minimizar sus puntos débiles.
- Simplificar al máximo el procedimiento administrativo cumpliendo con lo que está regulado por leyes, órdenes y normativas.
- Automatización de la mayor parte del procedimiento administrativo.
- Permitir al ciudadano entrar la mayoría de datos a los sistemas del Ayuntamiento.
- Dar valor al trabajo que el personal del Ayuntamiento realiza en el procedimiento administrativo.
- Maximizar la interoperabilidad.

Adicionalmente, durante la digitalización de procedimientos, la metodología deberá tener en cuenta que se analicen los siguientes aspectos, entre otros:

- La posibilidad de ejecutarlo telemáticamente y con el soporte de documentos electrónicos con validez jurídica.
- La posibilidad de utilizar declaraciones previas o declaraciones responsables por parte del ciudadano y el sentido del silencio administrativo.
- La racionalización de la información solicitada y la consideración de utilizar datos provenientes de otras Administraciones públicas sujetos a convenios de interoperabilidad.

- En relación a aquellos procedimientos que generan documentación que los ciudadanos entreguen a otras Administraciones públicas, analizar la posibilidad de entregarlos a través de medios telemáticos a la Administración pública solicitante, siempre sujeto a convenios de interoperabilidad.
- La automatización de tareas que actualmente se realizan de forma manual.
- Los usuarios que participan y la segregación de funciones así como las suplencias entre usuarios que puedan ser necesarias (bajas, suplencias, ...) con la finalidad de definir las políticas de acceso a documentos y expedientes. Estas políticas deberán definirse para cada tipo de documento y expediente y sus respectivas fases (activa, semiactiva e inactiva).
- La optimización del procedimiento: tareas superfluas que puedan eliminarse, tareas que gracias a herramientas informáticas ahora pueden realizarse de forma paralela, reorganización de las distintas fases. Por otro lado, si es necesario, considerar añadir tareas al procedimiento para facilitar su digitalización como por ejemplo el escaneo seguro de la documentación aportada por el ciudadano.
- Los documentos y plantillas que participan en el procedimiento y su racionalización con el objetivo de definir las políticas de firma.
- La identificación de los usuarios que necesitan certificado digital y la gestión de su ciclo de vida (creación, entrega, renovación, revocación,...).
- El uso de certificados digitales para la realización de tareas automáticas o que contemplen firmas automatizadas.
- La digitalización segura de documentos que participan en el proceso y están en soporte papel.
- La impresión segura de documentos electrónicos y garantizar el derecho del ciudadano a relacionarse con el Ayuntamiento a través de medios tradicionales, aunque el procedimiento del Ayuntamiento esté completamente en soporte electrónico.
- Notificaciones que se generan durante el procedimiento y posibilidades de practicarlas telemáticamente y con firma electrónica.

A modo de ejemplo de resultado de esta metodología, en el Anexo I se ha incluido un cuestionario útil para el análisis de procedimientos previo a su digitalización.

5.4 Metodología de aplicación del modelo a un expediente concreto

El Sistema de Gestión Documental tomará forma y será útil en la medida que se pueda poner en práctica para la gestión de documentos y expedientes concretos en soporte electrónico.

Los diferentes instrumentos que componen el Sistema de Gestión Documental definen con carácter general las reglas y criterios que se deben aplicar. Sin embargo, para convertir estos criterios en medidas de aplicación práctica, es necesario evaluar como los documentos que componen cada expediente en concreto deben ser tratados, a la vista de las reglas establecidas por el Sistema, y aprovechando el proceso de modelación y reingeniería.

El Ayuntamiento está trabajando en la progresiva automatización de los expedientes que gestiona, para muchos de los cuáles ya existen herramientas y soluciones que se apoyan en documentos electrónicos. Probablemente sería interesante empezar analizando estos casos concretos y evaluando si es necesario introducir alguna mejora en el tratamiento que actualmente se hace de estos documentos para alinearse mejor con el sistema.

Lo que se requiere, por tanto, es involucrar, en el proceso de modelación y reingeniería, a los responsables de archivo y gestión documental para que ayuden a elaborar un documento de aplicación del sistema de gestión documental al expediente electrónico correspondiente.

Este informe de aplicación debería contener, como mínimo, los siguientes puntos:

1. **Alcance:** Identificación de la tipología de expediente al que se hace referencia en el análisis.
2. **Caracterización del expediente:** En relación con el expediente, es necesario definir:
 2. a. **Apertura del expediente:** Identificar el momento o la acción que da lugar a la creación de un nuevo expediente de este tipo, y la manera como se identifican los documentos que deben ir asociados a él.
 2. b. **Clasificación del expediente:** Identificación del número de serie documental aplicable y las subdivisiones que puedan corresponder.
 2. c. **Ciclo de vida:** Descripción de las fases de vida del expediente: en qué momento se podrá cerrar el expediente, y a quién corresponde su cierre, y en qué momento se producirá la transferencia al archivo.
 2. d. **Evaluación y políticas de disposición:** Identificación de las tablas de retención que le sean aplicables y de la política de disposición que corresponda.
 2. e. **Criterios de acceso:** Determinación de los derechos de acceso al expediente, para cada una de las fases de vida (activa, semiactiva e histórica).

2. f. **Metadatos del expediente:** Aplicación en concreto del Vocabulario de Metadatos del Ayuntamiento, que permita determinar:

- Cuáles de los metadatos previstos tienen sentido para este tipo de expediente.
- Qué valor tomarán aquellos metadatos que tengan ya un valor fijo por pertenecer a esta serie documental, o que tomen su valor de un conjunto limitado.
- Cómo se determinará el valor de los demás metadatos.

3. **Documentos que componen el expediente:** En este punto se recomienda elaborar una tabla que identifique, para cada posible documento que pueda formar parte del expediente:

- Rol del documento en el expediente
- Tipología documental
- Propuesta de formato electrónico
- Obligatoriedad del documento en el expediente
- Cardinalidad
- Elementos de autenticidad (tipo de firma electrónica, elementos de evidencia, sello de tiempo, etc.)

Mediante la correlación entre tipologías documentales, formatos de documento electrónico y elementos de autenticidad se puede conseguir una mayor eficiencia en la implementación de procedimientos automatizados, al poder aprovechar a modo de arquetipos los desarrollos realizados para implementar otros documentos de características similares, aunque pudiesen pertenecer a expedientes radicalmente distintos.

Para cada uno de los documentos identificados será necesario identificar también:

- Los posibles valores que puedan tomar los metadatos aplicables.
- Los mecanismos de digitalización certificada, impresión segura o cambio de formato que puedan ser aplicables.

5.5 Responsabilidades en la aplicación de la Política Documental

El establecimiento, implementación, mantenimiento y mejora de un SGD es un reto de carácter transversal e interdisciplinar, de manera que precisa del trabajo cooperativo de profesionales que son expertos en los temas de su competencia pero que, usualmente, no tienen el hábito de trabajar conjuntamente y de manera concertada. El éxito de una implementación de un SGD se basa en una implicación directa de la alta dirección y de la formalización de una política de gestión de documentos que aglutine el esfuerzo planificado

de los profesionales de la organización bajo un lenguaje común. En el caso del Ayuntamiento es imprescindible la concurrencia de:

- La alta dirección, que debe impulsar el SGD y garantizar su sostenibilidad mediante la asignación de los recursos humanos y económicos adecuados.
- El Servicio de Tecnologías (ANIMSA) en tanto que responsable del modelo tecnológico de la organización.
- El Archivo Municipal, en tanto que Servicio de Archivo y Gestión de Documentos como órgano responsable de las políticas encaminadas a planificar, implementar y administrar un SGD.
- Los servicios jurídicos que deben garantizar la formalidad legal de los procesos y procedimientos.
- Los responsables de organización que se identifiquen, ya que deben liderar la modelación de los circuitos administrativos e impulsar la reingeniería de procesos.
- Los responsables de formación, que deben garantizar la difusión de la información necesaria para entender y aplicar las directrices del SGD y el conocimiento preciso de los instrumentos que lo desarrollan.
- El personal, de cualquier nivel, implicado en las tareas de gestión de documentos y que deberán aplicar el modelo a implantar en las acciones y trámites cotidianos y, en especial, mantener documentos precisos y completos de sus actividades, con la obligación de rendir cuentas de su quehacer.

Para fortalecer el proyecto y, sobre todo, coordinar las acciones que se planifiquen, se requiere la constitución de una Comisión Técnica de Gestión Documental, que garantice la continuidad del proyecto, su despliegue eficiente y la formalización de un calendario que permita asegurar una efectiva aplicación de los requerimientos del proyecto de manera secuencial y acumulativa.

Esta Comisión técnica de gestión documental estaría formada por dos personas designadas por el Archivo Municipal y dos representantes de ANIMSA, y tendría las siguientes funciones:

- Supervisar la formulación e implementación del Plan Director del Documento Electrónico
- Coordinar las acciones emprendidas durante el proceso de implementación
- Acordar las directrices y la normativa técnica necesaria para hacer efectiva la implementación
- Evaluar los recursos económicos y humanos necesarios

- Proceder a la valoración de la actualización tecnológica: decisión sobre formatos, y más concretamente decidir sobre su obsolescencia, sobre su migración y verificar su cumplimiento en un plazo no superior a tres meses.

Esta comisión se reunirá de manera periódica, elaborando en cada reunión acta de la misma.

En sintonía con las prescripciones contenidas en la norma ISO 15489-1: 2001 (6.3), es necesario definir las responsabilidades y competencias en el SGD, asignarlas y difundirlas, de manera que siempre que se identifique una necesidad específica de crear e incorporar documentos, sea posible determinar de manera inequívoca quien es el responsable de emprender la acción necesaria. Estas responsabilidades deben asignarse a todos los miembros de la organización y, muy especialmente, a los actores que acabamos de enumerar.

En particular, la definición de las responsabilidades, las competencias y sus interrelaciones han de permitir la aplicación de prácticas normalizadas y estandarizadas de manera que:

- Exijan a todos los miembros del personal la creación de documentos que respondan a las necesidades y a los procesos de negocio, con el objetivo de documentar de manera adecuada las actividades en que participen.
- Garanticen que los sistemas de información y de procesamiento que sirven de apoyo para las actividades de negocio permiten la creación de documentos apropiados como parte del apoyo a estas actividades.
- Aseguren la transparencia de los procesos documentales y la idoneidad del SGD a lo largo de toda su vida activa.
- Garanticen que los documentos se mantienen, se almacenan y se conservan durante todo el período que sean útiles para la organización y, cuando sea necesario, para público de interés externo como pueden ser instituciones archivísticas, investigadores y auditores.
- Asegurar que los documentos solamente se utilizan de conformidad con un proceso de aprobación definido previamente.

6. Modelo tecnológico del documento y expediente electrónico

La arquitectura tecnológica y sus interrelaciones para dar soporte a la gestión del documento y expediente electrónico han sido descritas en el apartado 3.6 de este Plan Director del Documento Electrónico. En relación con éste, el presente capítulo tiene por objetivo describir la participación de cada elemento tecnológico sobre las fases de tramitación y vigencia del ciclo de vida de los documentos electrónicos, considerándose, en su caso, la evaluación y destrucción de documentos y expedientes electrónicos.

A pesar de ello, cabe mencionar que en el capítulo 9 de este Plan Director, sobre el modelo de preservación de documentos electrónicos, se incluye mayor detalle sobre la gestión tecnológica de la fase histórica de los documentos y expedientes electrónicos y otros aspectos relacionados.

Adicionalmente, en este capítulo del Plan Director del Documento Electrónico se recogen las herramientas archivísticas de base para la gestión documental y la metodología para su construcción, concretamente: el Cuadro de Clasificación Documental, el Vocabulario de Metadatos, los Catálogos de tipologías y formatos documentales del Ayuntamiento y las Tablas de Evaluación Documental. Estas herramientas, constituyen los elementos de partida para la configuración de las herramientas tecnológicas que participan en el tratamiento de documentos electrónicos.

6.1 Representación del expediente y documento electrónico

Con carácter previo a describir como las herramientas tecnológicas de gestión documental del Ayuntamiento participan en el ciclo de vida de los documentos electrónicos es importante definir la representación de expediente y documento electrónico sobre el sistema de gestión de documentos electrónicos.

En este sentido, el sistema de gestión documental debe permitir el tratamiento unificado de expedientes y documentos electrónicos y de firmas electrónicas como objetos individualizables y de manera independiente a las herramientas de tramitación de expedientes. Su forma de representación estará constituida por:

- Los tipos de objeto: expediente, documento que forma parte de un expediente, documento independiente y firma electrónica.
- Metadatos asociados a cada tipo de objeto según el vocabulario de metadatos contenido en este capítulo.

La asociación de metadatos a cada tipo de objeto se realizará durante todo el ciclo de vida de los documentos electrónicos mediante las distintas herramientas tecnológicas que participen en su tratamiento y almacenamiento. En cualquier caso, todos los tipos de objetos serán almacenados junto con sus metadatos en el sistema de gestión de documentos electrónicos ALMADOC tal y como se describe a continuación.

6.2 El ciclo de vida de los documentos electrónicos en los entornos tecnológicos de gestión documental del Ayuntamiento

Partiendo de la arquitectura tecnológica de soporte a la gestión de documentos y expedientes electrónicos expuesta en el apartado 3.3 a nivel conceptual, el Ayuntamiento utiliza o tiene previsto utilizar las siguientes herramientas informáticas para dar soporte tecnológico al sistema de gestión de documentos y expedientes electrónicos:

- GEXP, desarrollada internamente, como herramienta de registro presencial y electrónico y de gestión de expedientes electrónicos
- ALMADOC, desarrollada internamente, como herramienta de gestión de documentos electrónicos en sus fases de tramitación y de vigencia.
 - o Nota importante: ALMADOC sólo almacena aquellos documentos que los usuarios responsables de la tramitación de expedientes consideren como definitivos o que deban formar parte del expediente los cuales, con carácter previo, son almacenados en un sistema de ficheros temporal accesible desde GEXP. Respecto a este sistema:
 - Queda fuera del alcance del modelo de gestión documental establecido por el presente Plan Director del Documento Electrónico, aunque deberá garantizar los mismos niveles de acceso que GEXP durante la fase de tramitación.
 - Es recomendable que, tras un tiempo prudencial después del cierre del expediente, se elimine de estos elementos accesorios toda documentación relacionada con el expediente con el objetivo de evitar duplicidades de información o el mantenimiento de información innecesaria.
- Herramienta de preservación de documentos y expedientes electrónicos a contratar e integrar con ALMADOC en base al modelo de duplicación de expedientes y documentos, según las directrices establecidas en el capítulo 9 de este Plan Director sobre el modelo de preservación.
- Herramienta web de consulta de expedientes y documentos electrónicos en fase de vigencia e histórica tal y como se describe en el apartado 6.2.4.

Con estos entornos tecnológicos se da cobertura completa al ciclo de vida de los documentos electrónicos según ha sido descrito en el apartado 3.3 de este Plan Director del Documento Electrónico. La participación concreta de cada entorno tecnológico en el sistema de gestión de documentos electrónicos se incluye a continuación organizado según sus distintas fases: tramitación, vigencia e histórica.

6.2.1 Fase de tramitación

La captura de documentos electrónicos en el sistema de gestión documental y, por lo tanto, el inicio del ciclo de vida de los documentos electrónicos puede producirse de las siguientes formas:

1. A través de entradas en la herramienta de registro de GEXP realizadas por el personal del Ayuntamiento y que deriven en el inicio de expedientes administrativos en la aplicación informática GEXP.
2. A través de trámites electrónicos disponibles en la Sede electrónica del Ayuntamiento que deriven en la anotación registral en GEXP y el consecuente inicio de expediente administrativo en GEXP.
3. En el inicio de expedientes de oficio directamente sobre el gestor de expedientes GEXP.
4. Durante la tramitación y resolución del expediente hasta su cierre y traspaso de responsabilidad al departamento de Archivo del Ayuntamiento.

Asimismo, durante el proceso de captura y el resto de fases del ciclo de vida del documento electrónico se producen las actuaciones, manuales y automáticas, sobre expedientes y documentos electrónicos que permiten:

- su clasificación según el Cuadro de Clasificación del Ayuntamiento y, en consecuencia, su evaluación según las Tablas de Evaluación Documental aprobadas por la Comisión Municipal de Evaluación Documental.
- su descripción según las normas internacionales (ISAD-G) e ISAAR-CPF y el Vocabulario de Metadatos del Ayuntamiento.
- su firma electrónica, si es requerida.
- identificar el tipo de documento al que corresponde según el Catálogo de tipologías documentales del Ayuntamiento.
- garantizar que los documentos estén o se conviertan a alguno de los formatos documentales aceptados según el Catálogo de formatos Ayuntamiento.

Estas cinco herramientas, básicas para la implementación del modelo tecnológico del documento y expediente electrónico, están contenidas en el tercer apartado 6.3 del presente capítulo del PDDE, exceptuando los aspectos relacionados con la firma electrónica para lo que debe consultarse el capítulo 11 sobre la Política de firma electrónica dentro de este Plan Director del Documento Electrónico. El resto de aspectos, relacionados con la captura de documentos en el sistema de gestión documental, son descritos a continuación.

6.2.1.1 Captura de documentos e inicio de expedientes a partir de la herramienta de registro

La incorporación de documentos provenientes de fuentes externas a la herramienta de registro de GEXP, sea presencialmente o telemática, comporta su captura en el sistema de gestión documental y da comienzo al ciclo de vida de los documentos electrónicos.

En caso de que los documentos incorporados estén en soporte no electrónico, para su captura en soporte electrónico será necesario aplicar procesos de digitalización tal y como se establece en el capítulo 7 sobre el modelo de digitalización segura y copia auténtica. Tras este proceso sólo se considerará documentación original en soporte electrónico aquella que se incorpore al registro, a través de:

- procedimientos de digitalización segura que generen documentos electrónicos firmados electrónicamente por el funcionario habilitado tras un proceso de careo entre el documento físico y el documento electrónico obtenido tras el proceso de digitalización.
- procedimientos de digitalización segura automatizada que haciendo uso de herramientas de digitalización certificada generen documentos electrónicos con firma electrónica de sello de órgano.

En el resto de casos, la documentación digitalizada se considerará copias de trabajo de documentos originales o no originales en papel.

En el caso que la documentación no pueda ser digitalizada se conservará el documento original en soporte papel y se introducirá un registro en ALMADOC, a través del gestor de expedientes correspondiente, incluyendo los metadatos relacionados, entre ellos, la ubicación física del documento en soporte papel. Con ello se posibilita la gestión de expedientes híbridos conformados de documentos tanto en soporte papel como electrónico.

En relación a la documentación aportada por el ciudadano a través de medios telemáticos, como es la tramitación electrónica accesible a través de la Sede electrónica del Ayuntamiento, se considerará original siempre que se trate de originales en soporte electrónico.

En el caso de documentación original en papel digitalizada por el ciudadano, El Ayuntamiento incorporará al expediente la copia resultante de la autocompulsión realizada por el ciudadano, reservándose el derecho a solicitar en cualquier momento la documentación física original, incluso si el ciudadano ha firmado electrónicamente estas copias. Si se produce dicha comprobación, el documento electrónico digitalizado por el ciudadano se completará con la firma del empleado público para reconocer su validez como copia auténtica fruto del careo entre el documento físico original y la imagen digital generada por el ciudadano.

Partiendo de las anotaciones realizadas en el registro de entradas y la documentación capturada, si GEXP dispone del correspondiente flujo de tramitación interna, una anotación

de registro de entradas permitirá el inicio, manual o automático, de uno o más expedientes o su vinculación a uno o más expedientes preexistentes considerándose lo siguiente:

- Durante la tramitación de un expediente se mantiene una única copia de un documento capturado independientemente del número de expedientes al que esté vinculado.
- No obstante, en el caso de un documento vinculado a más de un expediente en los siguientes casos se generará una copia del mismo con el objetivo de obtener un objeto digital único por expediente el cual incluya todos los documentos esenciales y obligatorios del expediente:
 - o Cuando se realicen modificaciones sobre el documento asociadas a un expediente en concreto se guardará una copia del documento incorporando las modificaciones vinculado al expediente en cuestión siguiendo el documento de partida, sin las modificaciones, vinculado al resto de expedientes sin incorporar dichas modificaciones.
 - o Cuando se determine su carácter de documento definitivo asociado a un expediente concreto, aunque no haya sufrido modificación alguna con respecto a ese expediente.

Para hacer posible el inicio de un expediente a partir de una anotación de registro de entradas, en aquellos casos que exista una modalidad de registro definida ésta estará unívocamente vinculada con una entrada del Cuadro de Clasificación del Ayuntamiento de manera que los documentos relacionados pueden clasificarse de acuerdo con el mismo y pueden vincularse a un procedimiento de gestión de expediente concreto. En caso contrario, se vinculará a una entrada del Cuadro de Clasificación temporal que será sustituida por la correspondiente en el momento que el destinatario de la entrada del registro atienda y clasifique debidamente la solicitud e inicie el expediente correspondiente o lo asocie a un expediente preexistente.

En ambos casos, el destinatario del registro será informado, mediante las funcionalidades de registro de GEXP, de la recepción de la entrada de registro y de los documentos relacionados siendo de su responsabilidad a partir de este momento:

- Comprobar que la introducción de metadatos sea correcta y, en su caso, completarla. Esta tarea resultará más o menos exigente en función de la calidad del proceso de captura.
- En el caso de que el documento haya sido vinculado a una entrada del Cuadro de Clasificación temporal, se procederá a clasificarlo definitivamente.
- Realizar, si aún no se ha hecho, la vinculación de la entrada de registro a un expediente preexistente o un nuevo expediente.
- Iniciar o dar continuidad a la tramitación del procedimiento asociado sobre GEXP.

La persona o departamento responsable deberá realizar estas actuaciones en un plazo inferior a 15 días. Si transcurrido este periodo no han sido realizadas se generarán avisos

a los responsables de tramitación solicitando la actuación correspondiente. Transcurridos 30 días sin que se haya realizado se generará un aviso a los responsables de archivo para que hagan seguimiento del caso.

Será necesario implementar controles específicos y realizar un seguimiento que garantice que no queden entradas de registro y documentos relacionados sin clasificar, es decir, en la entrada del Cuadro de Clasificación temporal.

Finalmente, una vez iniciada la tramitación de un expediente es importante señalar que podrán tener documentos relacionados con uno o más registros de salida y sus correspondientes documentos asociados.

6.2.1.2 Captura de documentos e inicio de expedientes de oficio sobre la herramienta de gestión de expedientes

Otra forma de iniciar expedientes, y la captura de documentos asociados al mismo, es el inicio de expedientes de oficio por parte del personal del Ayuntamiento directamente sobre la herramienta de gestión de expedientes GEXP sin la existencia de una entrada relacionada en el registro de entradas de GEXP.

En estos casos, los expedientes tendrán necesariamente asociada una entrada del cuadro de clasificación específica que en ningún caso corresponderá a una entrada temporal.

Este tipo de expedientes, como en el caso anterior, también podrán tener relacionados uno o más registros de salida y sus correspondientes documentos asociados.

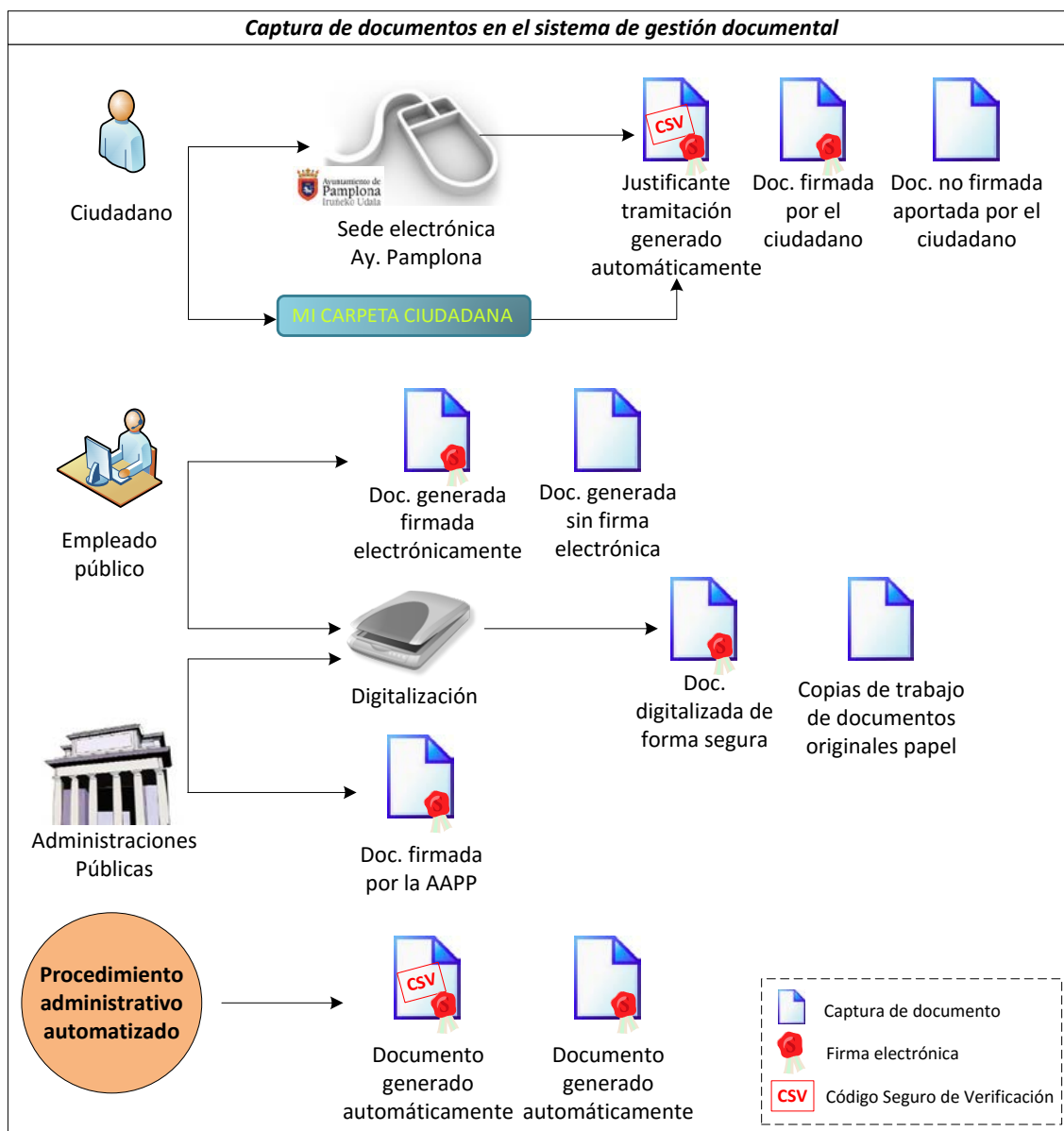
6.2.1.3 Captura de documentos durante la tramitación y resolución de expedientes

Una vez iniciado un expediente, también se producirá la captura de documentos electrónicos originales en el sistema de gestión de documentos y expedientes electrónicos y su asociación a uno o más expedientes, en los casos siguientes:

- Documentación generada durante el proceso de tramitación electrónica y que sea firmada electrónicamente por el ciudadano y/o por el ayuntamiento mediante procesos de firma automatizada, como son el formulario de tramitación y el justificante de registro electrónico, respectivamente.
- Documentación aportada por el ciudadano durante la tramitación electrónica que no incluya firma electrónica.
- Documentación generada o añadida durante la vida del expediente por el empleado público en cumplimiento de sus funciones, firmada o no firmada electrónicamente, con el objetivo de conformar el expediente con toda la documentación requerida según el tipo de procedimiento.

- Documentación digitalizada, sin firma electrónica, o digitalizada de forma segura incluyendo firma electrónica durante la vida del expediente por parte de los distintos departamentos del Ayuntamiento participantes.
- Documentación recibida a través de vías de interoperabilidad desde otras Administraciones Públicas y de relevancia para el expediente, ya sea incorporada manualmente o mediante procedimiento administrativo automatizado.
- Documentación generada a partir de un procedimiento administrativo automatizado, como por ejemplo los documentos de acuse de recibo generados durante el proceso de notificación electrónica o el documento de foliado del expediente.

A continuación, se incluye una representación gráfica de las distintas formas de captura de documentos en el sistema de gestión documental descritas en los anteriores subapartados:



6.2.1.4 Clasificación y descripción de documentos electrónicos

En el momento en que se realice una anotación en el registro de entradas y/o se inicie la tramitación de un expediente se producirá su clasificación, mediante el metadato correspondiente de expediente electrónico que permita su vinculación a una serie documental concreta establecida por el Cuadro de Clasificación del Ayuntamiento. Esta acción servirá además de base para establecer las políticas de seguridad y acceso tal y como se describe en el capítulo 10 de este PDDE sobre el modelo de seguridad.

Idealmente, esta asociación se debería producir en el momento de registro o, en su defecto, en el momento de inicio del expediente tal y como se ha descrito en los subapartados 6.2.1.1 y 6.2.1.2.

A pesar de ello, en los casos de:

- inicio de expediente a partir de una instancia general iniciada por el ciudadano a través de la Sede electrónica
- o de un registro de entrada en el que el funcionario de registro no tenga información suficiente para clasificar el expediente

Se prevé la posibilidad de que la clasificación se realice por parte del área responsable del expediente al mismo tiempo que inicia uno o más expedientes relacionados, pudiendo rechazarlo total o parcialmente por considerar no ser el área responsable. Para ello se utilizará una entrada temporal del Cuadro de Clasificación tal y como se ha expuesto en el subapartado 6.2.1.1.

Por lo que respecta a la captura de documentos quedarán vinculados con el expediente mediante el metadato correspondiente a número o números de expediente al que pertenecen.

Adicionalmente, durante todo el ciclo de vida del documento, expediente y firma electrónica se irán informando o modificando el valor de los metadatos que se recogen en el apartado 6.3.2 de este capítulo del PDDE. Tal y como se describe con mayor detenimiento en el apartado mencionado:

- la captura del valor de cada metadato se realizará tan pronto pueda ser conocido en las distintas fases del procedimiento de tramitación y, en la medida que sea posible, de forma automática o, en su defecto, se forzará al usuario a su introducción manual en el momento oportuno de la tramitación en que deba ser conocido evitándose, siempre que sea posible, la introducción libre del valor del metadato y primando listas de valores según define el vocabulario de metadatos.
- como mínimo se recogerá el valor de aquellos metadatos que deban ser informados de forma obligatoria según el Vocabulario de metadatos del Ayuntamiento.
- para cada nuevo procedimiento que se implemente en base a expedientes y documentos electrónicos se realizará un planteamiento sobre la forma específica de captura del valor de cada metadato tal y como se detalla en el apartado 6.4.

Por lo tanto, mediante estas acciones los documentos son capturados por el sistema de gestión documental asociados al expediente o expedientes correspondientes mediante el metadato de número de expediente, clasificados según el metadato del expediente sobre el punto del Cuadro de Clasificación al que pertenecen, evaluados según la Tabla de Evaluación correspondiente al punto del Cuadro de Clasificación y descritos según el valor de cada metadato que les corresponda.

6.2.1.5 Control de formatos del documento electrónico

Durante la tramitación del expediente los usuarios participantes indicarán a través del gestor de expedientes GEXP qué documentos pueden considerarse definitivos para proceder a su cambio de formato a PDF/A y su firma electrónica y qué otros, aunque no deban ser firmados electrónicamente, también deben formar parte del expediente definitivo manteniéndose su formato hasta el cierre del expediente. Sólo los documentos considerados definitivos conformarán el expediente una vez cerrado.

Mediante esta acción los documentos son capturados por el gestor documental ALMADOC asociados al expediente o expedientes correspondientes, clasificados según el metadato del expediente al que pertenecen y descritos según el valor de cada metadato que les corresponda. Con carácter previo los documentos habrán residido en el sistema de ficheros de GEXP.

Adicionalmente, en este proceso ALMADOC realiza un control de formatos de cada documento introducido y convierte de forma automática aquellos no aceptados a otros formatos aceptados según el catálogo de formatos del Ayuntamiento manteniendo, en cualquier caso, la forma y contenido del documento originario. Con carácter general los documentos serán transformados a formato PDF/A exceptuando documentos audiovisuales para los que se mantendrá el formato original tal y como se señala en el apartado 9.3 en el capítulo sobre el modelo de preservación.

6.2.2 Fase de vigencia

Una vez resuelto el expediente, el área responsable decide manualmente el momento oportuno para su cierre sobre GEXP o se determina de forma automática a partir de las acciones realizadas sobre el expediente o la información del mismo. El cierre del expediente desencadena los siguientes procesos automáticos:

- Verificación de que el expediente, antes de cerrarse, esté completo mediante la verificación de que el expediente en ALMADOC esté conformado por el número adecuado de documentos de aquellas tipologías documentales que corresponda según la Tabla de Evaluación Documental vinculada.
- Verificación de la completitud de firmas electrónicas y, en caso de que no estén completadas, se completarán automáticamente a los formatos requeridos según se

recoge en el capítulo 11 sobre el modelo de firma electrónica de este Plan Director del Documento Electrónico.

- Verificación de la completitud de metadatos de expediente, documento y firma electrónica según lo establecido por el Vocabulario de Metadatos del Ayuntamiento. En caso de que un metadato obligatorio deba ser informado o modificado y no pueda realizarse de forma automática se forzará su introducción por parte del usuario de tramitación según las directrices establecidas en el apartado 6.3.2 de este capítulo.
- Ampliación de permisos de acceso al expediente en cuestión en ALMADOC para que el personal responsable del Archivo del Ayuntamiento pueda revisar el expediente y aceptar o no su transferencia y, una vez aceptada, llevar a cabo las actuaciones relacionadas con la custodia y preservación. A partir del cierre del expediente la responsabilidad de su gestión pasa a recaer sobre el personal de Archivo y la documentación electrónica pasa a estar sujeta a las políticas de archivo y retención del Ayuntamiento. De la aceptación o denegación de la transferencia del expediente por parte del personal de Archivo, lo cual podrá realizarse individualmente o por grupos de expediente, quedarán las debidas constancias en ALMADOC según se describe en el capítulo 9 de este PDDE sobre el modelo de preservación.
- En ALMADOC se produce el foliado del expediente por el cual se genera un documento formato XML que se almacena directamente en ALMADOC vinculado al expediente y contiene:
 - o Metadatos de expediente.
 - o Índice de documentos que conforman el expediente, nombre del documento, descripción del documento y un resumen criptográfico de cada uno generado a partir de la función HASH SHA256.
 - o Firma automatizada con el sello de órgano del Ayuntamiento.

En el caso de tratarse de un expediente al que le aplique una Tabla de Evaluación Documental de eliminación parcial será necesario generar dos documentos de foliado del expediente; uno con los documentos requeridos en la fase de vigencia y otro con aquellos requeridos en la fase de archivo a largo plazo que se almacenarán según la temporalidad que establezca la Tabla de Evaluación Documental correspondiente. En estos casos deben estar inequívocamente identificados los documentos en los expedientes y poderse vincular a qué foliado deben formar parte según la Tabla de Evaluación Documental correspondiente.

En el caso de tratarse de un expediente sin Tabla de Evaluación Documental asociada, es decir, que sea por defecto de conservación permanente, en el momento en que se publique la TED y sea de eliminación parcial se aplicará a los expedientes futuros sin que se realicen actuaciones retroactivas relacionadas. El resto de posibilidades de evaluación documental, según son definidas en el

subapartado 6.3.5, podrán ser configuradas y aplicada a expedientes preexistentes contando con las funcionalidades propias del sistema.

Adicionalmente, ALMADOC dispondrá de las siguientes dos funcionalidades básicas entorno al foliado de expediente que también deberán contemplarse en la herramienta de archivo longevo:

- Un visor de ficheros XML que permita la interpretación humana del contenido de un foliado de expediente sin que ello suponga la generación de un nuevo expediente. Para ello deberá asociarse a cada fichero de foliado de expediente la hoja de estilo o plantilla de representación correspondiente que permita automatizar el proceso de interpretación.
 - Comprobación de la integridad de un expediente foliado por el cual se valide la integridad entre el contenido del fichero de foliado y documentación que lo conforma (mediante el recalcado del resumen criptográfico de cada documento). Ello permitirá dejar de aplicar medidas de preservación de la validez jurídica de los documentos que conforman el expediente para sólo aplicarlas al documento de foliado tal y como se detalla en el capítulo 7 sobre el modelo de preservación.
- Bloqueo de la edición del expediente en cuanto a sus datos y posibilidad de eliminar o añadir documentos.
 - Bloqueo de los metadatos descriptivos, que no deban sufrir modificaciones durante las fases de vigencia y archivo tal y como se identifica en el apartado 6.3.2.
 - Ampliación de permisos de acceso en GEXP para que el personal responsable del Archivo del Ayuntamiento pueda llevar a cabo las actuaciones relacionadas con la custodia y preservación.

Cabe mencionar que durante el proceso de cierre de un expediente no se realizan procedimientos de eliminación de documentos ya que sólo se consideran aquellos documentos seleccionados por los usuarios responsables de la tramitación conforme deban formar parte del expediente. Estos documentos habrán sido transferidos durante la tramitación del expediente, sin mantenerse copia, desde el elemento tecnológico accesorio de gestión de documentos, sistema de ficheros de GEXP, hasta el gestor documental ALMADOC.

En este sentido, cuando un documento está relacionado con distintos expedientes y se marca como definitivo para un expediente en concreto se mantiene copia del mismo en el elemento tecnológico accesorio de gestión de documentos. De esta forma, el documento, en el estado en que esté en ese momento, podrá seguir siendo utilizado en la tramitación de otros expedientes sucediéndose las modificaciones oportunas, si así es requerido.

A partir del cierre del expediente la responsabilidad de su gestión pasa a recaer sobre el personal de Archivo y la documentación electrónica pasa a estar sujeta a las políticas de archivo y retención del Ayuntamiento. Antes de ello, el personal de Archivo accede a GEXP para validar el expediente y aceptar o denegar su traspaso quedando las debidas

constancias en GEXP de la aceptación o denegación según se describe en el apartado 9.6 del capítulo de este PDDE sobre el modelo de preservación.

Una vez el personal de Archivo acepta la transferencia de un expediente, cualquier actuación sobre el mismo deberá ser realizada por los responsables de gestión documental y no por los responsables funcionales. No obstante, existirá la posibilidad, sólo en caso justificado, de que los responsables de gestión documental reabran el expediente a través de ALMADOC o la herramienta de archivo longevo, según donde se encuentre, para que los responsables funcionales puedan, mediante la aplicación de gestión del expediente correspondiente, añadir nueva documentación, nunca modificar o eliminar la existente.

Antes de ello, los responsables funcionales acceden a GEXP para aceptar o denegar la transferencia de responsabilidad sobre el expediente desde el personal de Archivo quedando las debidas constancias en GEXP de la aceptación o denegación según se describe en el apartado 9.6 del capítulo de este PDDE sobre el modelo de preservación.

Una vez finalizadas las actuaciones sobre el expediente reabierto se repetirá el proceso de cierre por el cual se realizará un nuevo proceso de foliado referente a la nueva situación de la información de metadatos de expediente, de los documentos preexistentes, incluyendo el foliado anterior, y los nuevos documentos añadidos considerados como definitivos.

Finalmente, durante la fase de vigencia, sin que el expediente, por no requerir de actuaciones de preservación, haya sido traspasado a la herramienta de preservación documental o archivo longevo puede suceder, en aplicación de la Tabla de Evaluación correspondiente, que se requiera de la eliminación completa o parcial del contenido del expediente. Estos procesos de eliminación se realizarán con el soporte de la herramienta ALMADOC o con la herramienta de archivo longevo, según donde estén los expedientes y tal y como se expone en el capítulo 9 de este PDDE sobre el modelo de preservación.

Para ello, en base a la Tabla de Evaluación Documental asociada a la serie documental a la que pertenezca un expediente, identificada mediante el valor del metadato correspondiente, el sistema que albergue el documento propondrá a los responsables de archivo las actuaciones de eliminación, total o parcial, que corresponda. Tras la aprobación por parte de los responsables de archivo, la herramienta en cuestión generará los registros de eliminación necesarios respetando las directrices al respecto de la Comisión Municipal de Evaluación Documental y guardando evidencia suficiente de la autorización del personal de Archivo.

6.2.3 Fase histórica

El ciclo de vida de los expedientes contemplará la posibilidad de transferencia de expedientes desde ALMADOC a una herramienta de archivo longevo para facilitar las tareas de preservación electrónica según se detalla en el capítulo 9 del modelo de preservación. A esta herramienta deberán almacenarse:

- En fase histórica: aquella documentación que sea de conservación permanente, es decir, pase a constituir patrimonio documental del Ayuntamiento, a partir del momento en que deje de ser consultada habitualmente por motivos administrativos y lo sea por motivos de investigación histórica. El período temporal habitual a transcurrir para ello será de 30 años y sólo se someterá a procesos de evaluación y destrucción en casos extraordinarios que serán decididos formalmente por la Comisión Técnica de Gestión Documental del Ayuntamiento.

En este caso, la documentación dejará de ser accesible a través de ALMADOC y, en consecuencia, de GEXP requiriéndose, en cualquier caso, para su acceso la solicitud al departamento de Archivo mediante la herramienta web que se detalla en el siguiente subapartado 6.2.4.

- En fase de vigencia: aquella documentación que, aunque no sea de conservación permanente, requiera de actuaciones de preservación en cuanto a su validez jurídica y legibilidad tal y como establece el modelo de preservación de documentos electrónicos a largo plazo en el capítulo 7 de este MGDE. Esta documentación sí estará sujeta a procesos de evaluación y destrucción en el entorno de la herramienta de preservación de documentos y expedientes electrónicos tal y como establecerá la Tabla de Evaluación Documental aplicable en cada caso.

En este caso, se mantendrá una copia de los documentos en ALMADOC en el estado en el que se encontraban previo a su transferencia al archivo longevo y que, por lo tanto, no recogerán las actuaciones de preservación realizadas de la herramienta de archivo longevo. No obstante, se identificará claramente que el documento original se encuentra ubicado en la herramienta de archivo longevo y que para su acceso deberá solicitarse al departamento de Archivo mediante la herramienta web detallada en el siguiente subapartado 6.2.4.

En ambos casos, los procesos de eliminación se cursarán de igual forma a como se ha indicado en el subapartado anterior 6.2.2 sobre la fase de vigencia de gestión documental, pero en este caso quedando en el sistema de archivo longevo las evidencias del proceso de eliminación y en ALMADOC las evidencias de transferencia del expediente al archivo longevo y de la autorización de la misma por parte del personal de Archivo.

Adicionalmente, la eliminación de documentación del sistema de archivo longevo supondrá también la eliminación de la copia de los documentos mantenida por ALMADOC correspondiente a la situación de la documentación en el momento previo a su traspaso a la herramienta de archivo.

Finalmente, debido a que reciben un mismo tratamiento, indistintamente a que pertenezcan a la fase de vigencia o histórica, se recogen en este mismo subapartado las actuaciones que realizará el personal de Archivo en aplicación del modelo de preservación que se contemplan en el capítulo 9 de este Plan Director. Estas actuaciones se realizarán con el soporte de la herramienta ALMADOC o con la herramienta de archivo longevo, según donde estén los expedientes, considerándose lo siguiente:

- ALMADOC guardará los metadatos de los expedientes traspasados a la herramienta de archivo longevo y de aquellos eliminados que serán accesibles desde GEXP sin que sea posible acceder a los documentos y firmas electrónicas y sus metadatos cuando hayan sido eliminados. La herramienta de archivo longevo también guardará copia de los metadatos de los expedientes recibidos aunque sean eliminados.
- ALMADOC, en base a la caducidad de la validez de la firma electrónica de un documento propondrá a los responsables de archivo su traspaso a la herramienta de archivo longevo a la que se delegan las actuaciones de preservación de la validez jurídica de los documentos electrónicos.
- Existirá la posibilidad de transferir un expediente a la herramienta de archivo longevo por motivo de la obsolescencia tecnológica del formato documental de uno o más documentos que lo conforman. Esta decisión será responsabilidad de la Comisión Técnica de Gestión Documental y será ejecutada sobre ALMADOC por parte del personal de Archivo. La herramienta de archivo longevo se encargará de realizar los procesos de migración de formatos correspondientes que garanticen la legibilidad de los documentos transferidos.
- La herramienta de archivo longevo en función del formato de los documentos y de la caducidad de las firmas electrónicas de los documentos de foliado de expediente identificará la necesidad de realización de:
 - o migración de formatos, lo cual deberá realizarse *ad hoc* para cada proceso de conversión y según lo establecido en el modelo de preservación en el capítulo 9 de este PDDE.
 - o procesos de resellado de tiempo, lo cual se realizará de forma automática dejando la debida constancia de ello en el sistema.

Para mayor detalle relacionado con la custodia y preservación de documentos consultar el capítulo 9 sobre el modelo de preservación.

6.2.4 Consulta de documentación en fase de vigencia e histórica

Tal y como establece el capítulo 10 de este PDDE sobre el modelo de seguridad, los usuarios que durante la fase de tramitación tuvieron acceso, restringido o confidencial, a la documentación traspasada al archivo seguirán manteniendo acceso a través de GEXP a la documentación:

- Que se encuentre en fase de vigencia y no haya sido traspasada a la herramienta de y no haya sido traspasada a la herramienta de archivo longevo.
- Que, pese a haber sido transferida a la herramienta de archivo longevo, una copia siga estando disponible en el sistema de gestión documental por los motivos descritos en el subapartado anterior.

Este acceso no conferirá ninguna posibilidad de edición de documentos o información asociada al expediente ya que, en cualquier caso, estará cerrado. De cada acceso se guardará constancia en un registro de accesos previsto a tal fin.

Adicionalmente, para el acceso a expedientes y documentos en fase de vigencia e histórica, podrán cursarse solicitudes de acceso al personal de Archivo del Ayuntamiento tanto por parte de usuarios internos, distintos a los que participaron en su tramitación, como externos. Por lo que respecta a las solicitudes de acceso de expedientes y documentos en fase de tramitación se resolverán por los responsables funcionales haciendo uso de las herramientas propias del gestor de expedientes correspondiente.

Para el inicio y gestión de solicitudes de acceso al departamento de Archivo existirá una herramienta web que permitirá a los usuarios internos autenticarse a partir de la Aplicación de Seguridad (ver capítulo 9 sobre el modelo de seguridad) y a los usuarios externos mediante certificado digital y cursar una solicitud al departamento de Archivo.

En las solicitudes de acceso deberá indicarse el valor concreto de un metadato o conjunto de ellos para que el personal de Archivo pueda resolver sobre la autorización de acceso a los expedientes relacionados. Existirá la posibilidad de que el personal de Archivo rechace la solicitud indicando los motivos que lo justifican o requiera mayor información para autorizar la misma lo que se generará una respuesta automática que será remitida al solicitante.

Las actuaciones realizadas por el personal de Archivo para resolver sobre solicitudes de acceso a expedientes y documentos electrónicos se realizarán sobre ALMADOC y, en su caso, sobre la herramienta de Archivo longevo pudiéndose definir sobre qué documentos se autoriza el acceso, el tiempo durante el cual este acceso será posible y si se permitirá la descarga o impresión de la documentación accedida. Con ello se generarán respuestas automáticas dirigidas al solicitante.

La resolución favorable del acceso se hará efectiva:

- en caso de usuarios internos, mediante accesos temporales a través de la herramienta de gestión de Expedientes GEXP si la documentación está ubicada en ALMADOC o, a través de la herramienta web si la documentación está ubicada en el Archivo longevo.
- en caso de usuarios externos o de usuarios internos sin experiencia sobre GEXP, indistintamente donde esté ubicada la documentación, mediante el acceso a la herramienta web mencionada que permitirá durante un período de tiempo limitado la consulta de la documentación.

Adicionalmente, en este caso, los accesos se realizarán durante el tiempo que autorice el personal de Archivo y sobre copias auténticas de los documentos firmadas con sello de órgano del Ayuntamiento, los cuáles incorporarán mención expresa de la temporalidad durante la cual será posible el acceso y permitirán, en caso de que los responsables de Archivo lo autoricen, su descarga o impresión. Estas copias se ubicarán en un repositorio documental temporal con las debidas

garantías de acceso y serán eliminados de forma automática una vez finalizado el plazo autorizado de acceso.

De todos los accesos que sucedan sobre la documentación tras la autorización de los responsables de Archivo quedará la debida constancia en el registro de accesos de la aplicación donde se ubique la documentación o la copia auténtica de la documentación accedida, identificándose la herramienta informática desde la que sucedió el acceso; GEXP o la herramienta web.

Adicionalmente, la herramienta web permitirá el acceso a aquella documentación calificada como de nivel de acceso público tanto a personal interno como usuarios externos o ciudadanía en general, indistintamente de la aplicación de gestión documental que los albergue (ALMADOC o herramienta de archivo longevo). De estos accesos no se requerirá obligatoriamente mantener un registro de accesos ya que los mismos podrían no quedar identificados la persona que los realiza.

Por otro lado, el personal de Archivo del Ayuntamiento tendrá los permisos suficientes para poder realizar, desde ALMADOC o la herramienta de archivo longevo, la exportación de un expediente, indistintamente de si el expediente está cerrado o abierto. Esta actuación podrá realizarse siempre que existan los motivos suficientes que fundamente la extracción de una copia de un expediente que tendrá por objeto ser entregada a usuarios distintos a los responsables funcionales o que hayan participado o tenido acceso durante la tramitación del expediente o a una tercera parte. De la extracción y de los motivos que la fundamentaron quedará la debida constancia en un registro de extracciones habilitado a tal fin en ambas herramientas donde será posible realizarlo.

Un expediente exportado contendrá:

- El documento de foliado del expediente, en caso de expediente cerrado ubicado en ALMADOC en fase de vigencia o la herramienta de archivo longevo, o el documento de foliado provisional del expediente, en caso de expediente abierto ubicado en ALMADOC en fase de tramitación.
- Los ficheros asociados al expediente sean documentos o firmas electrónicas asociadas a los mismos.
- Un documento con el resultado de la comprobación de la integridad del foliado del expediente resultado de la funcionalidad relacionada de ALMADOC o la herramienta de archivo longevo, según se identifica en el apartado 6.2.2.

6.3 Herramientas archivísticas de base y metodología para su construcción

En este apartado se identifican las herramientas de base para una adecuada gestión documental, independientemente de su soporte físico o electrónico, y se define sus características y criterios a tener en cuenta para su mantenimiento y evolución. Estas herramientas son:

- Cuadro de Clasificación
- Vocabulario de metadatos
- Catálogo de tipologías documentales
- Catálogo de formatos documentales
- Tablas de Evaluación Documental

La responsabilidad del mantenimiento de estas herramientas recae en el personal responsable del Archivo del Ayuntamiento sin perjuicio que el resto de miembros del Ayuntamiento puedan cursar solicitudes al departamento de Archivo para su modificación o ampliación.

6.3.1 Cuadro de clasificación: definición y mantenimiento de su estructura

El Cuadro de clasificación (Cuadro de Clasificación) permite agrupar jerárquicamente las series documentales en base a las funciones desarrolladas por el Ayuntamiento en el decurso de sus actividades, de acuerdo con los principios de procedencia y respecto al orden primitivo.

En este sentido, el Cuadro de Clasificación del Ayuntamiento es mayoritariamente de carácter uniforme y funcional, pero también está basado en los órganos ejecutores y se conforma mediante una estructura lógica y sistemática que refleja las funciones, las actividades o subfunciones, las series documentales y los expedientes que generan las distintas acciones y competencias que le son propias.

Cada uno de los niveles del Cuadro de Clasificación cuenta con un código de clasificación singularizado que es al mismo tiempo un metadato del expediente, concretamente el metadato eEMGDE22.1 - Código de clasificación según se recoge en el apartado 6.3.2. Ello permite que la estructura del Cuadro de Clasificación no deba ser implementada a nivel jerárquico en el sistema de gestión de documentos electrónicos sino que queda reflejada en un documento de carácter técnico cuyo desarrollo y mantenimiento depende del Departamento de Archivo del Ayuntamiento.

En la elaboración del Cuadro de Clasificación efectuada por el Departamento de Archivo del Ayuntamiento se ha seguido la metodología derivada de las directrices internacionales en la materia, especialmente la normativa del Consejo Internacional de Archivos, de la Mesa redonda de Archivos Municipales y del grupo de Archivos municipales de la Comunidad de Madrid. Asimismo, se ha seguido la práctica común en las organizaciones más avanzadas en esta materia las cuales han ido evolucionando desde unos postulados que componen un Cuadro de Clasificación asentado en la organización administrativa hacia un Cuadro de Clasificación basado en las funciones y actividades de la Organización y que constituyen un factor de estabilidad y continuidad en el tiempo.

El modelo utilizado para este Cuadro se fundamenta en los siguientes niveles:

- Primer nivel o Sección: denominación de la función. Es el nivel jerárquico inicial y no puede llevar adscrita ningún tipo de documentación.
- Segundo nivel o Subsección: subfunciones de la función. En el caso de no tener ningún desglose inferior podría llevar adscrita documentación.
- Tercer nivel o Grupo de Series: denominación de la actividad o subfunción o serie documental. En el caso de no tener ningún desglose inferior podría llevar adscrita documentación.
- Cuarto nivel o Serie: descripción detallada de la actividad o subfunción o serie documental específica y los expedientes que contiene.
- Quinto nivel: descripción de los expedientes que conforman una serie documental específica

Cada uno de los niveles cuenta con un código de clasificación que permite identificar automáticamente a qué nivel jerárquico del cuadro se está trabajando y qué tipo de documentación se le atribuye.

El Cuadro de Clasificación se considera una herramienta viva que evolucionará en el tiempo con tal de mantener su adecuación a las necesidades y funciones de la organización del Ayuntamiento, para su mantenimiento se procederá del siguiente modo:

- En el caso de procedimientos electrónicos, se identificará la serie o subserie documental correspondiente durante la fase de definición e implementación del procedimiento sobre las herramientas de gestión de expedientes electrónicos. En caso de no existir, el personal de Archivo creará una nueva serie o subserie documental dentro del Cuadro de Clasificación.
- En el caso de procedimientos basados en soporte papel, en el momento de transferencia al Archivo se identificará la serie o subserie documental que le corresponde y, en caso de no existir, el personal de Archivo creará una nueva serie o subserie documental dentro del Cuadro de Clasificación.

En ambos casos es posible que el punto del Cuadro de Clasificación al que pertenezca un procedimiento se haya identificado con carácter previo como resultado de la implementación de la gestión de expedientes sobre GEXP.

Para la creación de nuevas series o subseries se asignará la numeración consecutiva a la última que exista del grupo de series a la que pertenece. Por lo que respecta a la nomenclatura, se desarrollará un proceso de análisis conjunto entre el departamento de Archivo y el departamento responsable de los expedientes relacionados.

El documento que contiene actualizado el Cuadro de Clasificación del Ayuntamiento podrá consultarse en la Intranet del Ayuntamiento.

6.3.2 Vocabulario de metadatos: definición e implementación

Uno de los principales objetivos de la gestión de documentos, es poderlos localizar y consultar de forma sencilla y rápida y para ello es de vital importancia disponer de un conjunto de metadatos que permitan describir de la manera más eficiente posible el documento al que están asociadas. Adicionalmente, el procedimiento administrativo automatizado requiere de una estructura de datos homogénea para cada uno de los expedientes que facilite la automatización de tareas o la generación automática de documentos.

Por lo tanto, se requiere el uso de un vocabulario de metadatos que facilite la descripción de forma ordenada de todos los objetos a almacenar en el sistema de gestión documental: expediente, documento que forma parte de expediente, documento simple y firmas electrónicas asociadas a documentos.

El Ayuntamiento ha optado por la implantación del Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE) relacionado con la Norma Técnica de Interoperabilidad de la Política de gestión de documentos electrónicos con el objetivo de garantizar la interoperabilidad con otras Administraciones Públicas.

El e-EMGDE es accesible a través del Portal de Administración Electrónica del Gobierno de España. Este vocabulario de metadatos incorpora diferentes tipos de metadatos:

- Administrativos, hacen referencia a aspectos de gestión de los documentos electrónicos.
- Descriptivos, hacen referencia a aspectos de identificación e interpretación de los documentos electrónicos.
- Técnicos, hacen referencia a la captura, el formato, las dimensiones de las imágenes digitales, entre otros datos que pueden ser necesarias para asegurar el uso continuado de un objeto, o para reconstruir el objeto si se daña.
- Uso, hacen referencia a qué uso se ha hecho del documento.
- Preservación, estos son los metadatos que se necesitarán para mantener la validez y la representación del documento en cuestión.
- Clasificación / Acceso / Eliminación, metadatos que sitúan el documento dentro del marco global de la documentación administrativa del Ayuntamiento y que llevan asociadas las políticas, normativas y dictámenes establecidos sobre las series documentales.

Para la implementación de e-EMGDE es necesario determinar cómo se han de rellenar los metadatos que describen los objetos almacenados en el sistema de gestión de documentos electrónicos, para facilitar la búsqueda, consulta y gestión de documentos en todo momento.

Las fichas descriptivas de cada metadato, que se encuentran en el e-EMGDE, establecen las condiciones generales que deben cumplir cada uno de los metadatos, los criterios

utilizados para su generación y, en su caso, los posibles valores que pueden tomar. A pesar de ello, a continuación se describen las premisas que deberán respetarse a la hora de su implementación sobre las herramientas tecnológicas del ayuntamiento de gestión de documentos electrónicos:

- La captura de metadatos se hará siempre que sea posible de manera automatizada por las herramientas tecnológicas de gestión de documentos electrónicos y, en su defecto, estas herramientas forzarán a los usuarios, tanto internos como externos (ciudadanos), a que introduzcan el valor de metadato tan pronto como sea posible informarlo.
- Si durante el proceso de captura del documento no se han podido introducir todos los metadatos imprescindibles, éste no se podrá incorporar al expediente electrónico.
- Para la captura automática de metadatos las aplicaciones de gestión de documentos electrónicos emplearán:
 - o Datos del expediente almacenados en base de datos.
 - o Los permisos de acceso definidos sobre las herramientas de gestión de expedientes, desde donde se obtendrán los criterios de acceso a los documentos y su preservación.
 - o Datos de los certificados digitales utilizados para la firma de documentos, como por ejemplo los datos de identificación del firmante.
 - o Datos de la firma electrónica como por ejemplo el tipo, la fecha o el formato de la firma.
 - o Datos del sistema operativo como por ejemplo los de temporalidad (fecha y hora), el programa informático de creación y edición del documento que determinarán su formato o el tamaño del fichero que soporta el documento.
 - o De la "Aplicación de Seguridad" el nombre de usuario de sistema y su nombre completo, así como el departamento del Ayuntamiento al que pertenece y su cargo.
 - o Datos de la herramienta de registro GEXP como el número, la fecha y la hora y la modalidad de registro.
- Se establecerán patrones de generación automática de metadatos como por ejemplo en el caso de la numeración de expedientes conformada por la combinación de "Año + referencia Autonumérico" reiniciándose el contador cada año.
- En la definición de flujos de trabajo de expedientes y los documentos plantilla que se generarán se podrán definir valores por defecto de ciertos metadatos como por ejemplo la "Clasificación de sensibilidad de la LOPD". Se establecerán mecanismos sencillos de mantenimiento de esta información.

- De forma general se podrá aplicar el mismo valor de metadato por defecto para todos los documentos como por ejemplo el Código de Política de control de acceso dentro del grupo de metadatos referidos a la Clasificación de acceso.
- Los valores de ciertos metadatos podrán variar en el tiempo como es el ejemplo de “Estado de elaboración” de un documento.

Las premisas anteriores se establecerán mediante sistemas informáticos que permitirán determinar las condiciones necesarias para que el sistema actúe en cada caso según se pretenda para cada tipo de metadatos con la máxima automatización posible en cada caso.

Finalmente se incluye la siguiente tabla resumen en la que se identifican los metadatos utilizados por el Ayuntamiento basado en aquellos considerados obligatorios y aquellos opcionales relevantes para la gestión documental del Ayuntamiento, según el e-EMGDE. Adicionalmente, la siguiente tabla recoge para cada metadato:

- el código de vinculación con el e-EMGDE.
- su tipología: de descripción del elemento o para su gestión documental.
- su obligatoriedad, pudiendo ser condicional a otros elementos de gestión de metadatos.
- si son susceptibles de sufrir modificaciones una vez finalizada la fase de tramitación, es decir, durante las fases de vigencia e histórica.

Para mayor detalle nos referimos al e-EMGDE.

Metadato	Código e-EMGDE	Obligatoriedad	Tipología	Modificable tras fase de tramitación
eEMGDE0 TIPO DE ENTIDAD				
Tipo de entidad	eEMGDE0	Condiciona	Descripción	No
eEMGDE1 CATEGORÍA				
Categoría	eEMGDE1	Sí	Descripción	No
eEMGDE2 IDENTIFICADOR				
Secuencia de identificador	eEMGDE2.1	Sí	Descripción	No
Esquema de identificador	eEMGDE2.2	Condiciona	Gestión	No
eEMGDE3 NOMBRE				
Nombre natural	eEMGDE3.1	Condiciona	Descripción	No
Esquema de nombre	eEMGDE3.2	Condiciona	Gestión	No
eEMGDE4 FECHAS				
Fecha inicio	eEMGDE4.1	Sí	Gestión	No
eEMGDE5 DESCRIPCIÓN				
Descripción	eEMGDE5	No	Descripción	No
eEMGDE6 ENTIDAD RELACIONADA				
ID de entidad relacionada	eEMGDE6.1	Sí	Gestión	No
Esquema de ID de entidad relacionada	eEMGDE6.2	Condiciona	Gestión	No
Rol de la relación	eEMGDE6.3	Sí	Gestión	No
eEMGDE8 SEGURIDAD				
Clasificación de acceso (clasificación de acceso)	eEMGDE8.1.1	Condiciona	Gestión	Sí
Código de Política de control de acceso (clasificación de acceso)	eEMGDE8.1.2	Condiciona	Gestión	Sí
Permisos	eEMGDE8.3	Condiciona	Gestión	Sí
Sensibilidad datos de carácter personal	eEMGDE8.4	Condiciona	Gestión	No
Clasificación ENS	eEMGDE8.5	Condiciona	Gestión	No
eEMGDE9 DERECHOS DE ACCESO, USO Y REUTILIZACIÓN				
Condiciones de acceso, uso y reutilización	eEMGDE9.1	Condiciona	Gestión	Sí
Tipo de acceso	eEMGDE9.2	Condiciona	Gestión	Sí
eEMGDE10 CONTACTO				
Tipo de contacto	eEMGDE10.0	Condiciona	Gestión	No
Dato de contacto	eEMGDE10.2	Condiciona	Gestión	No
Puesto	eEMGDE10.3	Condiciona	Gestión	No
eEMGDE11 IDIOMA				
Idioma	eEMGDE11	Condiciona	Descripción	No
eEMGDE13 CALIFICACIÓN				
Valoración	eEMGDE13.1	Condiciona	Descripción	No
Tipo de dictamen (dictamen)	eEMGDE13.2.1	Condiciona	Descripción	No
Acción dictaminada (dictamen)	eEMGDE13.2.2	Condiciona	Descripción	No
eEMGDE14 CARACTERÍSTICAS TÉCNICAS				
Soporte origen	eEMGDE14.1	Sí	Descripción	No
Nombre de formato	eEMGDE14.2	Sí	Gestión	Sí

Metadato	Código e-EMGDE	Obligatoriedad	Tipología	Modificable tras fase de tramitación
Versión de formato	eEMGDE14.3	No	Gestión	Sí
Nombre de la aplicación de creación	eEMGDE14.4	Condicional	Gestión	No
Versión de la aplicación de creación	eEMGDE14.5	Condicional	Gestión	No
Registro de formatos	eEMGDE14.6	Condicional	Gestión	Sí
Resolución	eEMGDE14.7	Condicional	Gestión	No
Dimensiones físicas (tamaño)	eEMGDE14.8.1	Condicional	Gestión	No
Tamaño lógico (tamaño)	eEMGDE14.8.2	Condicional	Gestión	Sí
Cantidad (tamaño)	eEMGDE14.8.3	No	Gestión	No
Unidades (tamaño)	eEMGDE14.8.4	Condicional	Gestión	No
eEMGDE15 UBICACIÓN				
Soporte	eEMGDE15.1	Condicional	Gestión	No
Localización	eEMGDE15.2	No	Gestión	Sí
eEMGDE16 VERIFICACIÓN DE INTEGRIDAD				
Algoritmo	eEMGDE16.1	Condicional	Gestión	No
Valor	eEMGDE16.2	Condicional	Gestión	No
eEMGDE17 FIRMA				
Tipo de firma	eEMGDE17.1	Sí	Descripción	No
Formato de firma	eEMGDE17.2	Condicional	Gestión	No
Rol de firma	eEMGDE17.3	Condicional	Gestión	No
eEMGDE18 TIPO DOCUMENTAL				
Tipo documental	eEMGDE18	Sí	Descripción	No
eEMGDE20 ESTADO DE ELABORACIÓN				
Denominación del estado	eEMGDE20.1	Sí	Gestión	No
Características de la copia	eEMGDE20.2	Condicional	Gestión	Sí
Tipo de copia	eEMGDE20.3	Condicional	Gestión	Sí
Motivo	eEMGDE20.4	Condicional	Gestión	Sí
eEMGDE21 TRAZABILIDAD				
Acción	eEMGDE21.1	Condicional	Gestión	Sí
Motivo reglado	eEMGDE21.2	Condicional	Gestión	Sí
Usuario de la acción	eEMGDE21.3	Condicional	Gestión	Sí
Descripción	eEMGDE21.4	Condicional	Gestión	Sí
Modificación en los metadatos	eEMGDE21.5	Condicional	Gestión	Sí
Nombre del elemento (historia del cambio)	eEMGDE21.6.1	Condicional	Gestión	Sí
Valor anterior (historia del cambio)	eEMGDE21.6.2	Condicional	Gestión	Sí
eEMGDE21 CLASIFICACIÓN				
Código de clasificación	eEMGDE22.1	Condicional	Descripción	Sí
Denominación de clase	eEMGDE22.2	Condicional	Descripción	Sí

6.3.3 Catálogo de tipologías documentales

Existen multitud de tipologías de documentos empleados en el marco de la gestión administrativa y de la preservación de la memoria histórica relacionada con el ayuntamiento y el municipio de Pamplona.

Resulta necesario definir un catálogo o listado limitado de tipologías de documentos que establezca formalmente los tipos de documentos que el ayuntamiento reconoce y, a partir de los cuales, se podrán generar los documentos que participan en los procedimientos administrativos. Limitar el número de tipologías documentales permitirá las siguientes ventajas:

- Emplear plantillas estándares en la generación de los documentos del ayuntamiento y homogeneizar así el contenido y formato de los documentos administrativos.
- Establecer vínculos entre los tipos de documento y las diferentes fases del procedimiento administrativo controlando en cada una de estas fases qué tipos de documentos pueden ser generados.
- La delimitación estricta de los formatos documentales que deben apoyar cada tipología documental garantizando que se puedan aplicar medidas uniformes de cara a la gestión y preservación de la documentación, por ejemplo:
 - o el control automático de completitud de los documentos que conformarán un expediente concreto.
 - o el establecimiento de documentos que siempre deben de tener una o más firmas asociadas.

El catálogo de tipologías de documentos parte de la definida por el de la Universidad Pública de Navarra y el Grupo de Innovación Tecnológica del Departamento de Cultura y Medios de Comunicación de la Generalitat de Catalunya, y, además, se ha tenido en cuenta el Anexo I de la Norma Técnica de Interoperabilidad (NTI) del documento electrónico.

Dando cumplimiento a la NTI mencionada el catálogo de tipologías de documentos aceptados por el ayuntamiento se clasifican según sigue:

- **Documentos de decisión:** resoluciones, acuerdos, contratos, convenios, declaraciones, etc.
- **Documentos de transmisión:** comunicaciones, notificaciones, publicaciones, acuses de recibo, etc.
- **Documentos de constancia:** actas, certificaciones, diligencias, etc.
- **Documentos de juicio:** informes.
- **Documentos de ciudadano:** solicitudes, denuncias, alegaciones, recursos, facturas, etc.
- Otros.

Este catálogo estará vivo para ir adaptándose a lo largo del tiempo a las necesidades administrativas del Ayuntamiento. La última versión del catálogo de tipologías documentales del Ayuntamiento podrá consultarse en la Intranet del Ayuntamiento.

Finalmente, mencionar que el Catálogo de tipologías documentales del Ayuntamiento constituye el elemento de detalle del metadato "Tipo Documental" y deberá ser un metadato informado por defecto en plantillas de documentos o, en caso contrario, deberá ser informado por los usuarios del Ayuntamiento manualmente.

6.3.4 Catálogo de formatos documentales

La gran variedad de formatos de archivos informáticos existentes y la constante evolución tecnológica exige la definición de un catálogo de formatos documentales que delimite los formatos documentales aceptados por el Ayuntamiento que acabe revirtiendo en facilitar la gestión de documentos electrónicos.

Para la elaboración del catálogo de formatos documentales aceptados o normalizados por el Ayuntamiento se ha partido de la Norma Técnica de Interoperabilidad del Catálogo de estándares seleccionando aquellos que responden a:

- Formatos generalmente soportados por herramientas de preservación documental.
- La opinión y experiencia de los responsables de gestión de expedientes y de gestión documental o archivero del Ayuntamiento.
- Formatos abiertos (no propietarios, en la medida de lo posible).
- Formatos estándares, que disponen de la correspondiente definición como estándar internacional.
- Requerimientos de herramientas de archivo longevo (iArxiu, Baratz, STS, y otros – ver capítulo 9 del modelo de preservación) que faciliten la preservación a largo plazo de los documentos que participan en la gestión administrativa del ayuntamiento independientemente de su formato.

Para la aplicación del catálogo de formatos documentales sobre los procedimientos del Ayuntamiento se establecen tres directrices esenciales:

- Apuesta clara por el formato XML como estándar internacional y como conjunto de normas universales para la descripción de los datos y documentos. El uso del formato XML, conlleva la necesidad de implementar un proceso de vigilancia tecnológica para mantener la preservación de los elementos siguientes:
 - o La capacidad de leer y procesar elementos XML.
 - o La capacidad de almacenar, leer y procesar los diferentes esquemas concretos que definen contenidos en XML (por ejemplo, formatos de documentos de foliado de expediente electrónico o de facturación electrónica).

- La capacidad de producir transformaciones de los documentos XML a plantillas de representación aplicadas (por ejemplo, CSS, XHTML o XSLT).
- La capacidad de almacenar, leer y procesar las diferentes plantillas de representación aplicadas a las transformaciones de los documentos (por ejemplo, facturas electrónicas en formato facturae o documentos de foliado de expediente).
- Uso general del formato PDF/A definido en la ISO-19005. En este sentido, todo documento que pueda ser convertido a este formato lo será al cierre del expediente y, en caso contrario se utilizarán los siguientes formatos específicos:
 - Formatos audiovisuales: GIF, JPEG, TIFF y MPEG-4.
 - Diseños técnicos por ordenador: PDF/E (ISO 24517).
- Tener presente la tipología documental, según el formato, a gestionar en los procedimientos del Ayuntamiento primando el uso de cada formato según la finalidad para la cual fue concebido y la simplificación en cuanto al número de formatos utilizados.

Debido a la constante evolución tecnológica y su impacto en los formatos de archivos informáticos, el Catálogo de formatos documentales del Ayuntamiento se establece como un documento vivo cuya modificación requerirá de un proceso de reflexión para:

- En caso de ampliación se garantice la capacidad de los sistemas informáticos del Ayuntamiento en generar, custodiar y preservar documentos electrónicos bajo el nuevo formato.
- En caso de eliminación se ejecuten los procedimientos necesarios para garantizar las conversiones correspondientes de aquellos documentos ya existentes en el formato descatalogado.

A pesar de lo anterior, no será necesaria la modificación del Catálogo de formatos documentales y se podrán utilizar formatos distintos a los que en él se establecen siempre y cuando se trate de documentos volátiles, es decir, no tengan transcendencia en la gestión administrativa de expedientes ni deban ser preservados a largo plazo.

La última versión del catálogo de formatos de documentos electrónicos aceptados por el ayuntamiento se recoge en la siguiente tabla. Éste Catálogo se establece como el elemento de detalle del metadato "Nombre de formato" y deberá recogerse de forma automática a partir de las propiedades del fichero informático que soporte el documento electrónico.

Adicionalmente, en este Catálogo se incluye para cada formato el identificador asociado según la clasificación del registro técnico de formatos PRONOM perteneciente a los Archivos Nacionales de Inglaterra (The National Archives). En algunos casos el valor de este identificador puede no ser exactamente el que consta en un fichero informático de un formato determinado debido a la multitud de versiones existentes. No obstante, para obtener el identificador de formato PRONOM a partir de un fichero informático puede

consultarse la base de datos DROID a través del siguiente enlace:
<http://www.nationalarchives.gov.uk/information-management/our-services/dc-file-profiling-tool.htm>.

	Descripción del formato	Identificador PRONOM (PUID)
Documents de Texto		
	HTML (ISO/IEC 15445:2000)	fmt/100 y otros
	UTF encoded text (Unicode) (ISO/IEC 10646:2003)	fmt/51
	XML (ISO/IEC 13250-3:2007)	fmt/101 y otros
	XHTML (eXtensible HyperText Markup Language)	fmt/103 y otros
	Word 2007-2010	fmt/189
	Word 97-2003	fmt/40
	Word 2000 (9.0) for Windows	x-sfw/2
	Open Document Format (ISO/IEC 26300:2006)	fmt/135
Documentos Gráficos		
	JPEG2000 (ISO/IEC 15444)	fmt/43
	JPG (ISO/IEC 15444)	fmt/44
	PNG (ISO/IEC 15948:2004)	fmt/12
	PDF (ISO 32000-1:2008)	fmt/148 y otros
	PDF/A (ISO-19005)	fmt/95 (1a) fmt/354 (1b)
	TIFF (Tagged Image File Format - ISO 12639:2004)	fmt/353
	PDF/E (ISO 24517).	Description in preparation.
Documentos de Sonido		
	MP3 (ISO/IEC 11172)	fmt/134
Documentos de Video		
	MP4 (ISO/IEC 14496-14:2003)	fmt/357
	MPEG-4	fmt/199

6.3.5 Tablas de Evaluación Documental

Las Tablas de Evaluación Documental (TED) son un instrumento derivado de la aplicación de los criterios de evaluación de los documentos. La evaluación documental es una función destinada a determinar cuál es el valor de los documentos según sus usos administrativos, fiscales y jurídico-legales, tanto presentes como futuros, y su valor testimonial, informativo y de investigación o histórico, más orientados estos últimos a valorar la pertinencia de su conservación permanente.

El objetivo final de la evaluación documental es valorar cada una de las series documentales contenidas en el Cuadro de Clasificación del Ayuntamiento posibilitando la destrucción de aquellos documentos que, una vez cumplida la función que los generó, son

innecesarios para la gestión administrativa y la defensa jurídica y no tienen valores que aconsejen su conservación a futuro.

El Ayuntamiento constituirá una Comisión Técnica de Gestión Documental integrada por personal vinculado a los sectores de archivo y gestión documental, servicios jurídicos, servicios administrativos y el apoyo externo de un historiador contemporaneista.

Esta Comisión tiene dos objetivos fundamentales:

- Establecer formalmente los criterios y procedimientos para la evaluación y la destrucción documental y definir los registros de eliminación a mantener.
- Realizar un análisis exhaustivo de todas las series documentales del Cuadro de Clasificación del Ayuntamiento para determinar el valor de los documentos generados en relación a cada entrada del Cuadro de Clasificación y determinar su periodo de conservación a partir del cierre del expediente. Se considerarán las siguientes posibilidades de evaluación documental:
 - o Destrucción completa, identificándose los criterios o periodo sobre los cuales podrá realizarse la destrucción.
 - o Destrucción parcial, identificándose los criterios o periodo en base a los cuales se podrá determinar aquella documentación a destruir y a conservar dentro de un expediente y durante cuánto tiempo deberá conservarse la documentación no destruida.
 - o Destrucción por muestreo, determinándose los criterios en base a los cuales se seleccionan expedientes que se conservarán de manera permanente por motivos culturales o históricos, siendo eliminados los demás.
 - o Conservación permanente.

La evaluación de todas las entradas del Cuadro de Clasificación del Ayuntamiento constituirá un proceso prolongado en el tiempo. En este sentido, toda serie documental, mientras no sea evaluada, deberá considerarse de conservación permanente. Asimismo, para cada nueva entrada del Cuadro de Clasificación deberá realizarse un proceso de evaluación y para aquellas series evaluadas deberá realizarse un proceso de actualización en función de los cambios que sucedan al respecto.

Con el objetivo de contrastar los dictámenes de la Comisión Municipal de Evaluación Documental, éstos serán trasladados a la Comisión creada por el Gobierno de Navarra para su ratificación. Asimismo, durante los procesos de evaluación realizados por la Comisión Municipal se tomarán como referencia los dictámenes de la Comisión del Gobierno y otros organismos de referencia en este ámbito en aras a la homogeneización de criterios de evaluación.

Las Tablas de Evaluación Documental y su asociación a cada una de las entradas del Cuadro de Clasificación del Ayuntamiento podrán consultarse en la Intranet del Ayuntamiento.

6.4 Ficha de aplicación del modelo tecnológico del documento y expediente electrónico

La aplicación del modelo tecnológico del documento y expediente electrónico debe particularizarse a cada uno de los tipos de procedimientos del Ayuntamiento. En este apartado se recogen los aspectos necesarios de ser particularizados acompañándose de modelos de tablas útiles para llevarlo a cabo.

En relación a la generación de expedientes, es necesario identificar los criterios en función de los cuales se da inicio y fin a un expediente y la entrada del Cuadro de Clasificación con el que debe vincularse unívocamente el procedimiento que lo genera y, en consecuencia, a la Tabla de Evaluación correspondiente.

Procedimiento	Punto del Cuadro de Clasificación	TED	Criterios de inicio y fin de expedientes relacionados
Procedimiento 1			
Procedimiento...			

En relación a la documentación que participe en la vida de un expediente, es necesario identificar los documentos electrónicos que deban conformar un expediente durante su tramitación y en el momento de su foliado, así como a qué tipologías y formatos documentales responderán. Será de especial relevancia definir el contenido del documento de foliado como un documento más del expediente.

Documento que participa en el procedimiento de...	Tipología documental	Formato documental	Fase de tramitación en que es creado	¿Se elimina previo al foliado del expediente?
...				
Documento de Foliado				

En relación a la firma electrónica de documentos que participen en la vida de un expediente será necesario identificar:

- Qué flujo de firma se seguirá y qué número de firmas serán necesarias.
- Momento en el que deba generarse el flujo de firma electrónica durante el ciclo de vida del expediente y documento electrónico.
- Tipo (attached, detached,...) y formato de firma a realizar.
- Formato de las firmas.
- Nivel de firma: simple, paralela o anidada.

Documento firmado que participa en el procedimiento de...	Flujo de firma (cargo firmantes por orden de firma)	Momento de inicio del flujo firma	Tipo de firma	Formato de firma	Nivel de firma
...					

Documento firmado que participa en el procedimiento de...	Flujo de firma (cargo firmantes por orden de firma)	Momento de inicio del flujo firma	Tipo de firma	Formato de firma	Nivel de firma
Documento de Foliado					

A partir de aquí es necesario realizar un profundo análisis que permita identificar el mecanismo a seguir para la obtención del valor de los metadatos del expediente electrónico, los documentos electrónicos y las firmas electrónicas que participen durante el procedimiento hasta el cierre del expediente. Más concretamente para cada metadato será necesario especificar:

- Valor: si su valor está definido a nivel de todos los expedientes de la misma tipología y cuál es este valor o si su valor varía para cada expediente.
- Responsable de establecer su valor: en caso de que el valor no varíe, quien es el responsable de establecer su valor.
- Forma de informarla: en el caso de que el valor varíe, identificar cómo proceder para informarla, ya sea a partir del valor de otros metadatos o a partir de información contenida en el expediente o documento electrónico o en la firma electrónica o certificado digital que la genera. Ello podrá realizarse de forma automática por parte del sistema de gestión documental o de forma manual por parte de los usuarios del sistema.
- Momento de información o modificación: el momento en el ciclo de vida del expediente en que el valor se informa o se modifica.
- Observaciones útiles de cara a la recopilación del valor de cada metadato.

Metadato	Código e-EMGDE	Valor	Responsable de establecer su valor	Forma de informarla	Momento de información o modificación	Observaciones
eEMGDE0 TIPO DE ENTIDAD						
Tipo de entidad	eEMGDE0					
eEMGDE1 CATEGORÍA						
Categoría	eEMGDE1					
eEMGDE2 IDENTIFICADOR						
Secuencia de identificador	eEMGDE2.1					
Esquema de identificador	eEMGDE2.2					
eEMGDE3 NOMBRE						
Nombre natural	eEMGDE3.1					
Esquema de nombre	eEMGDE3.2					
eEMGDE4 FECHAS						
Fecha inicio	eEMGDE4.1					
eEMGDE5 DESCRIPCIÓN						

Metadato	Código e-EMGDE	Valor	Responsable de establecer su valor	Forma de informarla	Momento de información o modificación	Observaciones
Descripción	eEMGDE5					
eEMGDE6 ENTIDAD RELACIONADA						
ID de entidad relacionada	eEMGDE6.1					
Esquema de ID de entidad relacionada	eEMGDE6.2					
Rol de la relación	eEMGDE6.3					
eEMGDE8 SEGURIDAD						
Clasificación de acceso (clasificación de acceso)	eEMGDE8.1.1					
Código de Política de control de acceso (clasificación de acceso)	eEMGDE8.1.2					
Permisos	eEMGDE8.3					
Sensibilidad datos de carácter personal	eEMGDE8.4					
Clasificación ENS	eEMGDE8.5					
eEMGDE9 DERECHOS DE ACCESO, USO Y REUTILIZACIÓN						
Condiciones de acceso, uso y reutilización	eEMGDE9.1					
Tipo de acceso	eEMGDE9.2					
eEMGDE10 CONTACTO						
Tipo de contacto	eEMGDE10.0					
Dato de contacto	eEMGDE10.2					
Puesto	eEMGDE10.3					
eEMGDE11 IDIOMA						
Idioma	eEMGDE11					
eEMGDE13 CALIFICACIÓN						
Valoración	eEMGDE13.1					
Tipo de dictamen (dictamen)	eEMGDE13.2.1					
Acción dictaminada (dictamen)	eEMGDE13.2.2					
eEMGDE14 CARACTERÍSTICAS TÉCNICAS						
Soporte origen	eEMGDE14.1					
Nombre de formato	eEMGDE14.2					
Versión de formato	eEMGDE14.3					
Nombre de la aplicación de creación	eEMGDE14.4					
Versión de la aplicación de creación	eEMGDE14.5					
Registro de formatos	eEMGDE14.6					
Resolución	eEMGDE14.7					
Dimensiones físicas (tamaño)	eEMGDE14.8.1					

Metadato	Código e-EMGDE	Valor	Responsable de establecer su valor	Forma de informarla	Momento de información o modificación	Observaciones
Tamaño lógico (tamaño)	eEMGDE14.8.2					
Cantidad (tamaño)	eEMGDE14.8.3					
Unidades (tamaño)	eEMGDE14.8.4					
eEMGDE15 UBICACIÓN						
Soporte	eEMGDE15.1					
Localización	eEMGDE15.2					
eEMGDE16 VERIFICACIÓN DE INTEGRIDAD						
Algoritmo	eEMGDE16.1					
Valor	eEMGDE16.2					
eEMGDE17 FIRMA						
Tipo de firma	eEMGDE17.1					
Formato de firma	eEMGDE17.2					
Rol de firma	eEMGDE17.3					
eEMGDE18 TIPO DOCUMENTAL						
Tipo documental	eEMGDE18					
eEMGDE20 ESTADO DE ELABORACIÓN						
Denominación del estado	eEMGDE20.1					
Características de la copia	eEMGDE20.2					
Tipo de copia	eEMGDE20.3					
Motivo	eEMGDE20.4					
eEMGDE21 TRAZABILIDAD						
Acción	eEMGDE21.1					
Motivo reglado	eEMGDE21.2					
Usuario de la acción	eEMGDE21.3					
Descripción	eEMGDE21.4					
Modificación en los metadatos	eEMGDE21.5					
Nombre del elemento (historia del cambio)	eEMGDE21.6.1					
Valor anterior (historia del cambio)	eEMGDE21.6.2					
eEMGDE21 CLASIFICACIÓN						
Código de clasificación	eEMGDE22.1					
Denominación de clase	eEMGDE22.2					

7. Modelo de digitalización segura y copia auténtica

El modelo de gestión documental del Ayuntamiento de Pamplona está orientado a fomentar el uso del documento y expediente electrónico como herramienta principal en la gestión administrativa interna del Ayuntamiento.

Con la implementación sistemática de esta política se puede conseguir que los documentos que se generen en el Ayuntamiento nazcan en formato electrónico. Sin embargo, existirán siempre fuentes de documentación que lleguen al Ayuntamiento en soporte papel:

- Documentación generada por los ciudadanos, que tienen la opción de preferir el canal electrónico.
- Documentos aportados por los interesados, que al haber nacido en otro contexto pueden existir en soporte papel
- Documentos preexistentes en el Ayuntamiento, en expedientes en tramitación o incluso en expedientes cerrados, que pueda interesar digitalizar.
- Documentación que en casos puntuales se siga generando en soporte papel en el Ayuntamiento, sobre todo en el periodo transitorio mientras se acaba de desplegar esta política.

La legislación en materia de administración electrónica ha previsto la necesidad de poder incorporar la documentación de estos orígenes a los canales de tramitación electrónicos. Para ello es necesario digitalizar los documentos, ya sea como simples imágenes para facilitar su acceso, o como copias auténticas con plena validez que permiten eliminar el documento.

En este modelo estableceremos los mecanismos y procedimientos a través de los cuales se digitalizarán documentos en el Ayuntamiento.

7.1 Fundamento jurídico

La legislación que se ha aprobado en los últimos años tanto en el ámbito estatal como por el Gobierno de Navarra impulsa la implantación de una administración sin papeles, gestionada en base al uso de documentos electrónicos.

Sin embargo, en la puesta en práctica de este modelo hay que prever un largo período de convivencia de documentos electrónicos con documentos en papel. Aunque el Ayuntamiento haga un gran esfuerzo para implantar el documento electrónico de forma generalizada, no podemos pretender la desaparición total del papel:

- Por un lado, los administrados tienen, de acuerdo con lo establecido en la Ley 11/2007 y, a partir del 2 de octubre de 2016 según la ley 39/2015, la potestad de solicitar relacionarse con la administración en soporte papel. A pesar de que las personas jurídicas, las entidades sin personalidad jurídica, las personas físicas que ejerzan una actividad profesional de obligada colegiación, los

representantes de interesados obligados a relacionarse electrónicamente con la Administración y los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado están obligados a aceptar los intercambios electrónicos según el artículo 14 de la ley 39/2015, no podemos prever un escenario en el que se pueda dejar de admitir con carácter general la presentación de documentación en papel.

- Por otra parte, el proceso de modernización de otras organizaciones públicas puede ser desigual. El Ayuntamiento intercambia documentación con diferentes organizaciones dentro y fuera de Navarra, y mucha de esta documentación puede estar todavía en soporte papel.
- Finalmente, la propia pretensión que el Ayuntamiento pueda ser capaz de no generar documentación en papel es poco razonable a corto plazo, aunque sea el objetivo que nos planteamos en el horizonte.

Por estos motivos, es necesario prever soluciones para hacer compatible la gestión simultánea de documentación en soporte papel y en soporte electrónico. Por un lado, se contempla la existencia de expedientes híbridos, que podrán contener una parte de la documentación en electrónica y otra en papel, siempre que la lista de documentos que componen el expediente y sus metadatos estén correctamente identificadas en soporte electrónico en los sistemas de gestión documental.

Por otra parte, se contempla la digitalización como un mecanismo para incorporar documentos que se originen en papel los expedientes electrónicos. De esta manera, los documentos que lleguen al Ayuntamiento en soporte papel, o incluso aquellos que ya estén en expedientes en poder del Ayuntamiento, se pueden convertir en documentos electrónicos, incluso permitiendo la eliminación de los originales, tal como se describe en este modelo.

7.2 Escenarios de digitalización

El Esquema Nacional de Interoperabilidad, en su Anexo, apartado de glosario de términos, define la digitalización como "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 original".

Esta definición no requiere que la digitalización se haga a través de un procedimiento seguro. De hecho, podemos distinguir dos tipos de digitalización:

- La digitalización simple, que genera una imagen útil para la consulta pero que no se considera copia auténtica ni permite sustituir al original.

- La digitalización certificada, que genera un documento con valor de copia auténtica y puede permitir la destrucción del original. Dentro de este caso distinguimos dos escenarios:
 - Que la digitalización se haga de documentos que se presentan en el mostrador del registro de entrada y se devuelven al ciudadano á una vez hecha la captura. El documento en papel no llega a formar nunca parte de un expediente del Ayuntamiento.
 - Que la digitalización se haga de documentos que ya forman parte de un expediente del Ayuntamiento.

7.2.1 Digitalización Simple - Captura de imagen

La digitalización simple tiene como objetivo principal facilitar el acceso a la documentación a todas aquellas personas que lo necesiten para realizar sus tareas, por lo tanto, lo más importante es obtener una imagen del documento de forma rápida y ágil. La calidad de la imagen debe ser razonable y no será necesario garantizar su integridad y autenticidad, por lo tanto, no habría que firmarla, lo que agilizará el proceso de captura y consulta posterior, que son objetivos importantes para estos casos.

Las imágenes electrónicas suponen una herramienta muy útil para agilizar el acceso a la documentación y limitar el uso del papel. Sin embargo, hay que tener en cuenta que:

- a) Las imágenes electrónicas que no se han generado siguiendo un proceso de digitalización certificada no pueden sustituir la validez jurídica del original en papel.
- b) El proceso de digitalización es costoso en tiempo y recursos. Interesa, por tanto, garantizar que no se hacen digitalizaciones innecesarias.
- c) Los documentos digitalizados ocupan espacio en el sistema, y requieren de criterios de búsqueda para ser identificados más adelante. Este es otro motivo para limitar las digitalizaciones innecesarias.

Puede haber casos en los que, sin necesidad de hacer una digitalización segura, el Ayuntamiento puede estar interesado en obtener imágenes electrónicas simples para facilitar la gestión, tales como:

- a. Documentos de consulta masiva.
- b. Documentos presentados por un cliente o proveedor, sin valor legal, pero que interesa conservar el original y esta copia es suficiente para el Ayuntamiento.
- c. Documentos de vida muy corta, que solo interesan en la fase de tramitación.
- d. Documentos delicados que se conserven en soporte papel, pero se consultan a menudo y se podrían dañar.
- e. Documentos que se conservaran igualmente en soporte papel pero son de consulta frecuente.

En atención a estas consideraciones, se adoptan una serie de medidas para garantizar que no se malgastan esfuerzos en la digitalización de documentos.

- **Obtener una sola imagen de cada documento:** Para cada tipología de documento, o para cada procedimiento o trámite, se identificará en todo caso un único punto dentro del flujo de trabajo en el que se produzca la digitalización. El resto de participantes en el procedimiento deberán estar informados de dónde recae esta responsabilidad y, en caso de requerir la imagen del documento, solicitarla del responsable en lugar de generar una nueva.
- **Acceso al procedimiento debe implicar acceso a los documentos:** Cuando una persona dentro del Ayuntamiento obtenga una imagen electrónica de un documento, debe poder almacenarla en el gestor documental de tal manera que sea accesible para todas las personas que participarán en el procedimiento, asociando la imagen de manera clara con el procedimiento que le corresponda. Esto implica clasificarla y asociar los principales metadatos del expediente y documento, para facilitar su recuperación en un futuro.
- **Modificaciones en el documento no requieren obtener una nueva imagen:** Una vez que se ha obtenido una imagen electrónica de un documento, el hecho de que se hagan modificaciones menores en el documento no justifica la obtención de una nueva imagen, siempre que sea posible aportar esta información a través de anotaciones en el sistema de información asociado al expediente. Así, por ejemplo, el hecho de que un documento en estado borrador haya sido firmado definitivamente, se puede recoger con una anotación que indique la fecha de formalización del documento, sin que sea necesario obtener una nueva imagen.

Estas recomendaciones no serán de aplicación cuando la digitalización que se proponga cumpla con los requerimientos para generar copias auténticas que permitan la sustitución del original en papel.

7.2.1.1 Captura de imagen en el registro de entrada

El Registro de Entrada del Ayuntamiento de Pamplona tiene establecido un procedimiento en el registro de entrada de documentos, a través del cual a cada asiento de entrada se le puede asociar una imagen digitalizada del documento. Esta imagen se asocia al asiento de entrada.

En espera de que se pueda aplicar un procedimiento de digitalización segura en el registro de entrada, se introducen provisionalmente los siguientes cambios en el procedimiento existente, a fin de cumplir con las directrices establecidas en este apartado:

- a. Se digitalizará el documento entero, siempre que éste tenga 10 páginas o menos y no esté encuadernado o maquetado de tal manera que no se puedan separar las páginas de manera sencilla para su digitalización. En caso contrario, se digitalizará solo la primera página.

- b. La imagen resultante se almacenará en el gestor documental, en una carpeta de documentos asociados a las entradas de registro, identificada con el número de entrada de registro e indicando si es copia total o parcial.
- c. Cuando la persona responsable de tramitar la entrada de registro recupere el documento, lo asociará inmediatamente al expediente que le corresponda.

Estas medidas deberían permitir obtener copias de calidad de la mayoría de documentos sin generar una carga de trabajar excesiva al personal de registro.

7.2.1.2 Captura de imagen en los departamentos

Los Departamentos del Ayuntamiento podrán digitalizar documentos provenientes tanto del registro de entrada como de otras fuentes.

El procedimiento seguido será:

- a. Se digitalizará el documento entero.
- b. En el caso de documentos que hayan sido parcialmente digitalizados en el registro de entrada, se procederá a completar la digitalización.
- c. La imagen resultante se almacenará en el gestor documental, en la en una carpeta asociada al expediente al que pertenece el documento digitalizado.
- d. En el caso de documentos digitalizados en el registro, la persona responsable de tramitar la entrada de registro recupere el documento, lo asociará inmediatamente al expediente que le corresponda.

7.2.2 Digitalización segura o certificada

La Ley 11/2007, en su artículo 30 dice concretamente:

2. Las copias realizadas por las administraciones públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las administraciones públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la Ley 30 / 1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

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

Y la ley 39/2015, en vigor a partir del 2 de octubre de 2016, en su artículo 27 dice concretamente:

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

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

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

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

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

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

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

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

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

Por lo tanto, para que una copia electrónica tenga la consideración de copia auténtica y permita sustituir el soporte original, será necesario garantizar:

- La autenticidad del documento imagen.
- Su integridad.
- Su conservación.
- Incluir metadatos que acrediten su condición de copia y que se visualicen al consultar el documento. (artículo 27.3.a de la ley 39/2015)

El artículo 30 de la ley 11/2007 también hace una distinción entre dos escenarios:

- Artículo 30.2: copias de documentos emitidos por la administración pública en soporte papel. (a partir del 2 de octubre de 2016 éste escenario dejará de producirse según la ley 39/2015)
- Artículo 30.3: copias de documentos en papel aportados por el ciudadano.

Desde el punto de vista del procedimiento, tanto unas como otras se pueden obtener por procedimientos automáticos o con intervención humana. Desde el punto de vista del escenario, interesa hacer la distinción entre:

7.2.2.1 Compulsa electrónica a la entrada de documentos

El Ayuntamiento de Pamplona habilitará un procedimiento para que los documentos que los ciudadanos y las empresas aportan al registro de entrada en soporte papel puedan ser digitalizados de manera segura, de tal manera que lo único que se incorpore al expediente sea el documento electrónico.

Como se ha indicado más arriba, de manera provisional la digitalización de documentos en la entrada se hará sin medidas adicionales de seguridad. Cuando se disponga de los recursos humanos y tecnológicos se pondrá en funcionamiento uno de los dos procedimientos que se describen a continuación:

a. Compulsa electrónica en el registro con intervención humana:

En este caso, el personal de registro realizará las mismas tareas que se han descrito en el apartado 7.2.1.1, con las siguientes modificaciones:

- Los documentos sujetos a digitalización completa serán todos los que cumplan los criterios siguientes:
 - Deben formar parte del expediente en el momento del foliado de éste.
 - Tienen validez jurídica
 - Pueden ser necesarios para complementar la evidencia de un acto ante un conflicto, ya sea éste interno o externo.
 - Los documentos que previamente no hubieran sido digitalizados de forma segura y localizables para ser incorporados al expediente.
- La copia electrónica resultante será firmada por el técnico de registro, debidamente habilitado, con su certificado electrónico, de la manera que se describe en el apartado 7.5.1 de Digitalización Manual.

Los documentos que se hayan digitalizado de esta manera se podrán devolver al ciudadano. Sólo se conservarán en soporte papel los documentos que no hayan cumplido los requerimientos para ser digitalizados.

b. Compulsa electrónica en los departamentos o archivo con intervención humana:

En este caso, el personal de registro realizará las mismas tareas que se han descrito en el apartado 7.2.1.2, con las siguientes modificaciones:

- Los documentos sujetos a digitalización completa serán todos los que cumplan los criterios siguientes:
 - Deben formar parte del expediente en el momento del foliado de éste.
 - Tienen validez jurídica
 - Pueden ser necesarios para complementar la evidencia de un acto ante un conflicto, ya sea éste interno o externo.
 - Los documentos que previamente no hubieran sido digitalizados de forma segura y localizables para ser incorporados al expediente.
- La copia electrónica resultante será firmada por el técnico del departamento o del archivo, debidamente habilitado, de la manera que se describe en el apartado 7.5.1 de Digitalización Manual.

Los documentos que se hayan digitalizado de esta manera se podrán devolver al ciudadano. Sólo se conservarán en soporte papel los documentos que no hayan cumplido los requerimientos para ser digitalizados.

c. Compulsa electrónica automatizada:

En este caso, tanto el personal de registro como los departamentos y archivo dispondrán de hardware adecuado para la digitalización automatizada, y de un sistema de impresión de código de barras, como se describe en detalle en el apartado 7.5.4 de Digitalización para etiquetado.

- Los documentos sujetos a digitalización completa serán todos los que cumplan los criterios siguientes:
 - Deben formar parte del expediente en el momento del foliado de éste.
 - Tienen validez jurídica
 - Pueden ser necesarios para complementar la evidencia de un acto ante un conflicto, ya sea éste interno o externo.
 - Los documentos que previamente no hubieran sido digitalizados de forma segura y localizables para ser incorporados al expediente.
- En relación con estos documentos, los que se gestionen desde el registro, se generará un código de barras que los relacionará con su entrada de registro y que se pegará en un lugar del documento o no se oculte la información contenida en la primera página, o se aprovechará el código que incorpore el propio formulario, en su caso.

- Estos documentos etiquetados se acumularán en una bandeja auxiliar, para ser alimentados en el sistema de digitalización automatizada. Este sistema aplicará las medidas de seguridad descritas en el apartado 7.5.3 y asociará el documento resultante a su entrada de registro.
- Los documentos que no hayan sido etiquetados se digitalizarán de igual forma, y se aplicarán las medidas de seguridad descritas en el apartado 7.5.3.

Los documentos que se hayan digitalizado de esta manera se podrán devolver al ciudadano, que deberá venir a recogerlos el siguiente día laborable. Sólo se conservarán en soporte papel los documentos que no hayan cumplido los requerimientos para ser digitalizados.

7.2.2.2 Digitalización interna

Este es el escenario en que un departamento del Ayuntamiento, o bien los responsables de archivo, deciden digitalizar uno o más documentos o expedientes que ya están incorporados, en formato papel, en la gestión interna del Ayuntamiento.

En este caso habrá que definir un proyecto de digitalización de documentos, tal como se describe en el Anexo II, y aplicar un proceso de digitalización segura (probablemente automatizada como se describe en el apartado 7.5.2 o externalizada, como se describe en el apartado 7.5.4).

7.3 Procedimiento de digitalización Segura

Teniendo en cuenta el objeto y alcance de este Modelo, se considera digitalización segura el proceso regulado de captura de información de un material en soporte no digital, que incorpora una serie de medidas de seguridad y legalidad que garantizan que el documento electrónico resultante corresponde al material original capturado y puede ser tratado como copia auténtica con las consecuencias previstas por la Ley 11/2007 y, a partir del 2 de octubre de 2016, la ley 39/2015.

Por tanto, los principales objetivos perseguidos a la hora de seleccionar un método de digitalización seguro serán:

- Asegurar un valor probatorio pleno del documento digitalizado sobre los hechos o actos que documente, equivalente al documento original.
- Garantizar la fiabilidad del documento digitalizado como evidencia electrónica de la actividad o procedimiento correspondiente según lo dispuesto en el artículo 21 del RD 4/2010 ENI.
- Avalar la autenticidad del documento digitalizado mediante las medidas de seguridad definidas en el RD 3/2010 NOS y lo dispuesto en el artículo 22 del RD 4/2010 ENI.

- Permitir la destrucción del documento en soporte papel en el momento que se establezca por parte de la Comisión de Acceso, Evaluación y Selección Documental atendiendo a la legislación y normativa aplicable.

La digitalización certificada se caracteriza por una serie de requerimientos de seguridad, que se pueden alcanzar de dos maneras:

- Mediante una plataforma de digitalización automatizada.
- A través de la intervención de una persona adecuadamente formada, que garantice con su firma la identidad de la imagen obtenida con el original.
- Adicionalmente, contemplan la posibilidad de que la digitalización pueda subcontratar a una empresa especializada, que aplique procedimientos de digitalización automatizada siguiendo las directrices establecidas por el Ayuntamiento.

7.3.1 Documentación a digitalizar

El procedimiento de digitalización segura de los documentos en soporte papel se aplicará a los documentos o series documentales que pertenezcan a cualquiera de las siguientes categorías:

- Documentación administrativa en fase activa, semiactiva o inactiva. Cualquier documento en soporte papel que forme parte de un expediente administrativo es objeto de ser digitalizado de forma segura.
- Documentación aportada por los ciudadanos a un procedimiento administrativo cuando no exista la necesidad de que los originales consten en el expediente administrativo.
- Cualquier documentación interna, no administrativa, que obre en poder del Ayuntamiento, que requiera unos requisitos de seguridad y / o legalidad.
- Cualquier documentación científica y de investigación que requiera ser intercambiada con otras administraciones.

7.3.2 Escenarios en los que aplica

El procedimiento que se describe a continuación explica en detalle todos los requerimientos para que un proyecto de digitalización se lleve a cabo con todas las garantías. Esto puede aplicarse tanto a:

- Digitalización interna de documentación existente en los expedientes del Ayuntamiento.
- Digitalización de documentación en el registro de entrada.

En el segundo caso, todas las referencias en preparación, autorización y documentación del proyecto se entenderán hechas en el procedimiento de actuación del registro, que una vez establecido y aprobado se aplicará de manera sistemática sin más requerimientos formales.

7.4 Requisitos del proceso de digitalización

En este punto se establecen los requisitos de proceso de digitalización segura agrupados en:

- Procedimientos necesarios;
- Requisitos técnicos;
- Requisitos de la imagen electrónica;
- Seguridad;
- Otros requisitos jurídicos.

7.4.1 Procedimientos necesarios

A continuación, se identifican los procedimientos que deben implementarse en el Ayuntamiento cuando se desee realizar un proceso de digitalización segura:

PROCEDIMIENTO	DESCRIPCIÓN
AUTORIZACIÓN Y APROBACIÓN DEL PROCESO DE DIGITALIZACIÓN	Documento de alto nivel (política) que define el alcance y la motivación de la digitalización e Incluye el proceso formal de autorización.
DOCUMENTACIÓN DEL PROYECTO	Cuando se lance un proyecto de digitalización, habrá que documentar a qué documentación aplica y como se llevará a cabo de entre las posibilidades identificadas en el apartado 7.5.
PRESTACIÓN DEL SERVICIO POR EL PROPIO AYUNTAMIENTO O CONTRATACIÓN DE UN SERVICIO EXTERNO	En caso de externalización del servicio de digitalización será necesario incluir ciertas cláusulas particulares en el contrato entre el Ayuntamiento y el proveedor tal y como se establece en el apartado 7.5.4.

PROCEDIMIENTO		DESCRIPCIÓN
FORMACIÓN DEL PERSONAL IMPLICADO EN LA DIGITALIZACIÓN		Todo agente involucrado en el proceso de digitalización debe contar con los conocimientos necesarios que garanticen su aptitud tanto técnica como organizativa para realizar correctamente su función. En caso de externalización del servicio este requisito se contemplará a nivel contractual tal y como se establece en el apartado 7.5.4.
PROCESO TECNOLÓGICO		Se define en el apartado 7.5.
SEGURIDAD	Creación y mantenimiento de copias maestras de documentos digitalizados	El tratamiento de las copias maestras requiere un procedimiento que englobe desde su creación hasta su destrucción en base a las políticas de gestión documental y de seguridad existentes.
	Copias de Seguridad	El procedimiento de copias de seguridad atenderá a lo establecido al efecto en el modelo de seguridad del documento electrónico del Ayuntamiento, apartado 10 del PDDE.
EVALUACIÓN DOCUMENTAL	Conservación de los documentos	Procedimiento que incluye la estrategia de conservación de los documentos digitalizados sobre la base de las políticas de gestión documental y de seguridad existentes.

PROCEDIMIENTO		DESCRIPCIÓN
	Disposición de los documentos originales	Aquellos documentos que no sean restituidos a sus titulares tras la digitalización, se someterán a las políticas de conservación de documentos del Ayuntamiento según establece su modelo de preservación, apartado 9 del PDDE. Previa aprobación de la Comisión Técnica de Gestión Documental, se podrán eliminar los originales en papel una vez está suficientemente garantizada la conservación de las copias resultantes del proceso de digitalización.
	Disposición los documentos digitalizados	La valoración y la disposición de los documentos originales deberá ser procedimentada sobre la base de las políticas de gestión documental y de seguridad existentes.

7.4.2 Requerimientos técnicos

La NTI establece una serie de requisitos técnicos que deben cumplirse para garantizar la calidad del procedimiento de digitalización. En el Anexo III se especifican en detalle estos requerimientos.

7.4.3 Seguridad

A la hora de abordar las medidas de seguridad a tener en cuenta en el proceso de digitalización segura, se observará lo siguiente:

- La Política de Seguridad del Ayuntamiento, así como su desarrollo normativo.
- Los aspectos concretos relacionados con la política de firma electrónica basada en certificados que están recogidos en el Modelo de Firma Electrónica.
- Las medidas de seguridad referenciadas en el Esquema Nacional de Seguridad (ENS). Los sistemas de información que soportan el proceso de digitalización segura deberán cumplir con las exigencias del ENS.

La implantación de estas medidas en los sistemas de información deberá estar condicionada a la valoración del nivel de seguridad en cada dimensión de seguridad, y en la categoría del sistema de información de que se trate.

Se prestará especial atención para garantizar que el control de acceso físico y lógico a la información que maneje el personal implicado en el proceso de digitalización sea el mínimo requerido para el desempeño de sus funciones.

Se recomienda llevar una trazabilidad de los accesos a los diferentes activos de información implicados. Para esta tarea se podrán utilizar los metadatos específicos de trazabilidad.

7.4.4 Otros requisitos jurídicos

Habrá que dotarse de una norma específica que regule todos los elementos jurídicos que certifiquen la validez del proceso de digitalización. Entre ellos, tratará los siguientes aspectos:

- **Protección de datos.** Aspectos fundamentales a tener en cuenta para el cumplimiento de la normativa de protección de datos personales que se ha convertido en un punto esencial en la gestión de documentos electrónicos y especialmente en procesos de digitalización de documentación sensible.
- **Estándares.** Cuestiones como el cumplimiento de los principios de accesibilidad y usabilidad de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.
- **Mecanismos de habilitación.** Identificación de los procedimientos de habilitación que requiera el proceso de digitalización, enmarcado, en todo caso, en las políticas o reglamentos internos existentes en el Ayuntamiento.
- **Protección de la propiedad intelectual.** Cuando se digitalicen obras con copyright se deberá establecer un control de acceso adecuado.
- **Otros requisitos,** como aquellos específicos para llevar a cabo una copia, requisitos de autenticidad, requisitos de los tipos de copias, etc.

7.5 Ejecución de la Digitalización

7.5.1 Digitalización Manual

La ley 11/2007 y, a partir del 2 de octubre de 2016, la ley 39/2015 prevé la posibilidad de que la calidad e integridad de la imagen generada sea validada por un trabajador público habilitado al efecto. El resto de requerimientos relacionados con la seguridad y custodia de la imagen generada se deben cumplir en todo caso.

En este caso, por tanto, no es imprescindible disponer de hardware y software específicamente homologado, pero sí que hay que cumplir con los siguientes requerimientos en el proceso de digitalización:

- El proceso de escaneo se debe realizar por medios fotoeléctricos, utilizando un dispositivo de captura, el cual genera un archivo imagen, al que se aplican los procesos de optimización que se consideren adecuados.
- La imagen se pone a disposición de un usuario habilitado, que la compara con el original en papel para garantizar la identidad. Para garantizar la integridad y autenticidad de la imagen, una vez hecha la comprobación la firma con su certificado digital.
- El documento imagen se deberá completar con los metadatos correspondientes, a fin de generar un documento electrónico completo. Normalmente, en el proceso con intervención humana, esta carga de metadatos se hará manualmente.
- Las condiciones técnicas y requerimientos para la generación y verificación de las firmas, serán las establecidas por las normativas correspondientes.
- El certificado digital a emplear será preferiblemente el personal del trabajador que realiza la comprobación, aunque sería aceptable utilizar un sello de órgano, hechas las habilitaciones correspondientes.

A partir de aquí, el documento sigue el mismo proceso que en la digitalización automatizada, y se deberá incorporar un sistema de gestión documental adecuadamente preparado para garantizar la correcta clasificación y gestión del documento resultante.

7.5.2 Digitalización Automatizada

Una digitalización segura automatizada se obtiene empleando una plataforma compuesta por un dispositivo de captura de la imagen, más los drivers / controladores necesarios para comunicarse con ellos y un software que sea capaz de generar un archivo que contendrá la imagen digital del documento original en formato papel. Además, para asegurar una reproducción fiel e íntegra del documento digitalizado, será necesario acreditar que la imagen digital se ha obtenido mediante un proceso automático sin interrupción y sin intervención de ninguna persona física, en línea a lo establecido en la Resolución de 24 de octubre de 2007 de la Agencia Estatal de Administración Tributaria, sobre el procedimiento para la homologación de software de digitalización contemplado en la Orden EHA / 962/2007, de 10 de abril de 2007.

Concretamente la plataforma para la digitalización certificada, deberá cumplir los siguientes requerimientos:

- El proceso de escaneo se debe realizar por medios fotoeléctricos, utilizando un dispositivo de captura, el cual genera un fichero que queda en la memoria del

sistema asociado al dispositivo, sin interrupciones y sin la intervención de ninguna persona física.

- A continuación, se aplica el proceso de optimización de la imagen, con el fin de obtener una imagen con mayor calidad; se pueden usar softwares específicos, que deberán estar firmados digitalmente por el fabricante (para garantizar que no se han producido manipulaciones).
- Firma de la imagen del documento digitalizado, para garantizar su integridad y autenticidad.
- La aplicación de creación de firma debe estar incorporada al escáner como driver. De esta forma se puede asegurar que la imagen se firma antes de que el archivo se grabe en el disco, o sea que todo se hace en el espacio de memoria del equipo en cuestión. Hay que tener en cuenta un pequeño cambio en esta funcionalidad en el caso del cotejo, ya que será necesaria la aceptación por parte de la persona trabajadora de la administración pública, que realiza la comparación entre la imagen digital y el documento original, antes de firmar con el correspondiente certificado digital de trabajador/a público/a.
- En aquellos casos que sea necesaria la intervención humana, la aplicación deberá disponer de mecanismos estrictos de seguridad que permitan guardar pruebas de todas las acciones realizadas (trazabilidad).
- Hay que vincular el archivo de imagen en los metadatos técnicos, ya sea a través de una estructura de archivo. xml o a través de la inserción de los metadatos en base de datos o en el gestor documental.
- Las condiciones técnicas y requerimientos para la generación y verificación de las firmas, serán las establecidas por las normativas correspondientes.
- Los certificados digitales a emplear en procesos automatizados y desatendidos será un sello de órgano o un certificado de hardware, como un sello electrónico de la FNMT.
- El documento digitalizado se deberá incorporar a un sistema de gestión documental adecuadamente preparado para garantizar la correcta clasificación y gestión del documento resultante.

El software deberá cumplir las siguientes características:

- El proceso de captura debe garantizar una imagen fiel e íntegra de cada documento, firmada electrónicamente, así como la organización de la documentación en una base de datos documental.
- El software debe generar documentos en alguno de los formatos incluidos en el catálogo de formatos identificado en el apartado 7.6.
- El nivel de resolución debe ser como mínimo 200 ppp.

- El medio empleado para la digitalización debe ser fotoeléctrico.
- La calidad de la imagen capturada se debe optimizar.

Por tanto, todo proceso de digitalización de documentos podría ser considerado digitalización certificada, siempre que cumpla con los requerimientos enumerados en los párrafos anteriores. Concretamente, la Guía de Aplicación de la Norma Técnica de Interoperabilidad de "Digitalización de Documentos", establece unos requerimientos mínimos a cumplir por la imagen resultante de la digitalización, los que se añadirán aquellos que se consideren necesarios para garantizar su fidelidad de la imagen y la integridad del archivo electrónico resultante.

7.5.3 Digitalización mediante etiquetado

Este es un caso particular de digitalización automatizada, que el Ayuntamiento podrá utilizar en el contexto de la digitalización de documentos que se presentan en el registro de entrada.

En este caso, el personal de registro, en el momento de recibir la documentación, crea un asentamiento de registro donde se identifican los datos habituales de registro del documento. Esto permite al sistema informático crear un identificador único para el documento, a la espera de su recepción a través de mecanismos de digitalización.

Cuando la carga de trabajo o los recursos tecnológicos no permitan la inmediata digitalización manual del documento, lo que se hará será imprimir una etiqueta con un código de barras que identifique el número único del documento, el número de páginas de que se compone y si contiene información por ambas caras o no.

En determinadas ocasiones, el documento que se presente a registro ya incorpora el código de barras, porque ha sido generado a partir de una aplicación de generación de formularios que lo prevé, en cuyo caso no será necesario incorporar la etiqueta.

El documento, etiquetado con el código de barras, se guardará en una bandeja para su digitalización automatizada y el sistema de captura automáticamente identificará, a través de la etiqueta, el conjunto de páginas que forman un documento, y la ubicación en el gestor documental donde se debe almacenar.

7.5.4 Digitalización externalizada

La digitalización externalizada, responde a aquellos procesos de digitalización que no se pueden abordar por falta de recursos internos, y por tanto se decide subcontratar a un proveedor externo especializado con este tipo de trabajos, para poder hacerlo.

Para obtener unas imágenes electrónicas de los documentos originales en soporte papel, con el máximo de garantías, será necesario redactar un contrato en el que se establecerá un procedimiento estricto y detallado, en el que se describan todas las tareas a realizar,

concretando al máximo como se llevarán a cabo, incluyendo un riguroso control de calidad y unas medidas de seguridad estrictas para garantizar al máximo la calidad, confidencialidad e integridad. Además, es imprescindible que se mantenga trazabilidad de todo el proceso, anotando el máximo de información de todas y cada una de las tareas realizadas.

Ambas partes firmarán este contrato, en el que el Ayuntamiento y la empresa tercera hacen constar por escrito las condiciones que regirán la relación, concretando los derechos y deberes de cada una de las partes.

Los aspectos imprescindibles que debería incluir este contrato se describen en detalle en el Anexo IV.

7.6 Formatos de digitalización

El formato de archivo para las imágenes electrónicas deberá cumplir con los requisitos de resolución, profundidad de bits, información de color y metadatos que se definan. Para su elección, deberá asegurarse de que cumplirán lo establecido al efecto en la *NTI de Catálogo de Estándares*.

A continuación, se muestra el listado de formatos que pueden ser utilizados en la digitalización segura. Para cada uno de ellos, se incluyen los siguientes atributos:

- **Formato:** nombre del formato.
- **Versión:** versión mínima considerada.
- **Extensión:** listado de extensiones de archivo.
- **Tipo:** estándar abierto o estándar de facto.
- **Profundidad de bits:** bitonal / escala de grises a x bits / color a x bits.
- **Compresión:** compresión con pérdida / compresión sin pérdida.
- **Gestión del color:** RGB / YCb Cr / CMYK / Otros.
- **Soporte metadatos:** sí / no.

La admisibilidad o selección de otros formatos no reflejados en esta tabla, deberán atender a las condiciones establecidas en el artículo 11 del R.D. 4/2010 ENI.

Se destaca en color el formato preferido por el Ayuntamiento.

Formato	versión	ext.	Tipo	Profundidad de bits	Compresión	Gestión del color	Soporte metadatos
GIF	GIF 89a	.gif	Estándares de facto	Bitonal. Escala de grises: de 4 a 8 bits. Color de 4 a 8 bits.	Sin pérdida: LZW.	Paleta propia	S í (campo de texto libre).
JPEG	ISO / IEC 15444	.jpg .jpeg	Estándares abierto	Escala de grises a 8 bits. Color a 24 bits.	Sin pérdida: JFIF Con pérdida.	Y C _b C _r	S í (campo de texto libre).
PDF- PDF / A	ISO 32000-1: 2008 ISO 19005-1: 2005 y 2011 (PDF / A).	.pdf	Estándares abierto	Escala de grises a 4 bits. Color de 8 hasta 64 bits.	Sin pérdida: ITU-T.6, LZW Con pérdida: JPEG	RGB Y C _b C _r CMYK	S í (conjunto básico).
PNG	ISO / IEC 15948: 2004	.png	Estándares abierto	Escala de grises de 8 a 16 bits. Color de 8 a 48 bits.	Sin pérdida: Deflate, derivado de LZ77.	sRGB ICC	S í (conjunto básico más rótulos definidos por el usuario).
TIFF	ISO 12639: 2004	.tiff .tif	Estándares abierto	Bitonal. Escala de grises: de 4 a 8 bits. Color de 8 a 64 bits.	Sin pérdida: LZW.	RGB Y C _b C _r CMYK CIE L * a * b *	S í (encabezamiento de archivo).

Listado de formatos admitidos para la digitalización segura.

7.7 Metadatos de digitalización segura

Los metadatos que son de aplicación a las copias auténticas de documentos en papel que se generen en el marco de las actividades del Ayuntamiento, y que se deberán añadir a los identificados el vocabulario de metadatos del Ayuntamiento, que se ha definido en el apartado sobre Modelo Tecnológico, se relacionan a continuación:

Elemento	Metadato	Definición
eEMGDE14.1	Soporte origen	Valor: Papel

eEMGDE14.4	Nombre de la aplicación de creación	Denominación del software utilizado para la digitalización del documento papel.
eEMGDE 14.5	Versión de la aplicación de creación	Versión de la aplicación de creación
eEMGDE 14.7	Resolución	Valor de resolución en píxeles per pulgada empleada en la digitalización.
eEMGDE 20.2	Característica de la copia	Información sobre las características de la copia.
eEMGDE 20.2.1	Tipo de copia	Obligatorio en todo caso con el valor: "Copia electrónica auténtica de documento papel"
eEMGDE 20.2.2	Motivo	Descripción del motivo por el que se ha hecho la copia.
eEMGDE21	Trazabilidad	Incorporar toda la información referente a la persona o procedimiento administrativo automatizado que ha realizado el proceso de copia.

7.8 Habilitación de la digitalización

7.8.1 Elementos tecnológicos

Por lo que se ha estado explicando en esta política, los elementos tecnológicos necesarios son dos, un escáner y el software que se encarga de generar la imagen electrónica del documento original en soporte papel.

El software y el escáner, son dos elementos intrínsecamente relacionados, ya que uno sin el otro no permitiría obtener una imagen electrónica correcta del documento a digitalizar en soporte papel.

A la hora de seleccionar el dispositivo de captura, se tendrán en cuenta los siguientes criterios, ordenados por prioridad:

- Velocidad de captura
- Área de exploración
- Automatización y adaptación al soporte documental
- Rendimiento de captura en resolución tonal / color
- Rendimiento de captura en resolución espacial
- Uniformidad de captura

- Tratamiento de imagen automatizado
- Configuración de formatos de salida
- Configuración de compresiones
- Posibilidad de aplicación de tecnología OCR (en soporte textual)
- Generación de metadatos automatizado
- Coste

En este entorno se emplean algunos conceptos muy específicos del mundo de la digitalización, que a continuación se define, también se incluyen otros conceptos relacionados con la digitalización, aunque no se hayan usado en este documento.

Controlador de escáner: El controlador del escáner, conocido también popularmente como driver, es el programa que permite iniciar y parametrizar el proceso de captura. La mayoría de veces, este programa es proporcionado por el mismo proveedor del escáner. Aunque la mayoría de máquinas permiten el uso de otros controladores más avanzados, generalmente el programa que lleva por defecto el escáner suele ser el que mejor se adapta a sus posibilidades. El controlador permite configurar numerosas opciones de la captura, como el área de exploración, la resolución espacial, la tonalidad, la profundidad de color, el formato de salida, etc. Hoy, los controladores más avanzados incluso permiten hacer retoque gráfico de la imagen digital dentro del mismo proceso de captura.

En caso de que nos interese realizar digitalización certificada, el mismo controlador de escáner debería ser capaz de firmar el documento en el mismo procedimiento de captura, en caso de que no se firmen los documentos directamente al almacenarlos en su ubicación destino.

Controlador TWAIN: TWAIN es una interfaz de programa estándar mediante la cual los programas gráficos y de captura pueden comunicarse con dispositivos que proporcionan datos gráficos. Es decir, esta interfaz permite ejecutar la orden de captura directamente desde el programa de procesamiento de la imagen digital sin tener que manipular la máquina.

Visores: Los visores son programas especializados en la presentación de las imágenes digitales, ya sea en la pantalla como a través de su impresión. Estos programas integrados con los dispositivos que deben permitir la verificación de la captura por parte del equipo de trabajo y en el ordenador del usuario final que tiene que recuperar la información.

Los visores deben permitir realizar numerosas operaciones sobre la imagen digital, con el fin de poder captar con detalle y modificarla según convenga:

- Selección del área de impresión o visualización
- Zoom (acercamiento o distanciamiento de la imagen)
- Rotación y / o inversión (efecto espejo)

- Desplazamiento de la zona visible de la imagen cuando esta es más grande que la superficie de la pantalla
- Ajuste del brillo, del contraste, del color y la resolución.

Editores de imagen digital: Entendiendo por imagen digital, como la conversión de un documento analógico a digital, tendremos que ampliar los límites de la edición del documento de imagen fija también el del documento de imagen en movimiento y sonoro. En general, estos editores tienen la capacidad de manipular los parámetros de calidad y las características del documento digital capturado. Entre la multitud de funcionalidades que puede desarrollar un editor avanzado de imagen digital destacamos las siguientes:

- Control del dispositivo de captura, así como la posibilidad de ajustar los parámetros de estos dispositivos en el proceso de conversión. Asimismo, permite controlar los dispositivos de impresión y ajustar también sus parámetros de salida.
- Gestión del formato de la imagen digital, así como su compresión, monitorización (impresión, visualización o audición) y grabación en dispositivos de almacenamiento.
- Síntesis de imágenes con la posibilidad de crear archivos nuevos a partir de estas.
- Modificación de las características y aspecto de las imágenes a través del ajuste de la resolución espacial, la profundidad de bit, la tonalidad, etc. La edición también permite la superposición de capas de información, ya sea gráfica o sonora, según el tipo de documento que se trate.

7.8.2 Habilitación jurídica

La habilitación jurídica que da cobertura legal al proceso de digitalización se soporta fundamentalmente en dos elementos:

- La aprobación del Plan Director del Documento Electrónico.
- La documentación específica de cada proyecto de digitalización, para el que el área responsable de la serie documental, conjuntamente con los responsables tecnológicos y los responsables de archivo, definirán en un documento los términos en que se hará la digitalización de aquella documentación en concreto.
 - En el caso de la documentación que accede al Ayuntamiento a través del registro de entrada, se hará una única regulación de carácter general.

8. Modelo de impresión segura

El modelo de gestión documental del Ayuntamiento de Pamplona está orientado a fomentar el uso del documento y expediente electrónico como herramienta principal en la gestión administrativa interna del Ayuntamiento.

Pese a esta apuesta firme por el uso de estas tecnologías, este modelo documental no puede ignorar que existirán personas y entidades que se relacionarán con el Ayuntamiento y no dispondrán de las herramientas necesarias para utilizar de manera eficaz los documentos electrónicos. Incluso a largo plazo se prevé la necesidad de poder entregar a los interesados copias en papel de los documentos administrativos que les afecten, y que dichas copias en papel tengan validez jurídica plena.

La legislación en materia de administración electrónica, y en concreto la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, específicamente recoge el derecho de los ciudadanos a relacionarse con la administración por canales no electrónicos (artículos 4.b. y 27.1). A partir del 2 de octubre de 2016, éste derecho para la mayoría de personas físicas se recogerá en el artículo 14 de la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas. Esta opción del ciudadano hace referencia al intercambio de documentación e información entre la administración y los interesados, pero en ningún caso debe condicionar el soporte en el que se conduzca la actividad administrativa en el seno del Ayuntamiento.

Para conjugar la voluntad de la administración de utilizar preferentemente documentos electrónicos, con el derecho del ciudadano a recibirlos en soporte papel, la ley prevé la posibilidad de poder generar copias auténticas en formato papel de documentos originales en soporte electrónico. A continuación, se describen los mecanismos a través de los cuales el Ayuntamiento utilizará esta posibilidad.

8.1 Fundamento jurídico

El artículo 30.5 de la Ley 11/2007 y, a partir del 2 de octubre de 2016, los artículos 27.3.c) y 27.3.d) de la ley 39/2015 da cobertura al procedimiento de impresión segura, a través del cual se pueden generar copias en papel de documentos originalmente emitidos en soporte electrónico. El requisito legal para que estas copias tengan valor de copia auténtica es que incorporen **un código generado electrónicamente** u otro mecanismo de verificación que permita contrastar su autenticidad mediante el acceso a los archivos electrónicos del Ayuntamiento.

A este Código Seguro de Verificación (CSV) se hace referencia también en el artículo 18.1.b) de la Ley 11/2007 y, a partir del 2 de octubre de 2016 en el artículo 42.b) de la ley 40/2015 se establece como el mecanismo a través del cual se puede comprobar la integridad de un documento impreso mediante su cotejo con el documento electrónico correspondiente mediante el acceso a la sede electrónica del Ayuntamiento.

La Ley Foral 11/2007 también establece, en su artículo 9.5, que *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*, cosa que concuerda con la necesidad de permitir la identificación de los documentos impresos con su original electrónico de la manera que se describe en esta Ley.

La Norma Técnica de Interoperabilidad sobre copiado auténtico y conversión de documentos electrónicos, aprobada por Resolución de la Secretaría de Estado para la Función Pública de 19 de julio de 2011, recoge esta posibilidad en su apartado VII, remitiéndose directamente al resto de la normativa aplicable.

El objeto, por tanto, del uso de un mecanismo de impresión segura ha de ser el de generar una copia, cuando el ciudadano lo necesite, del documento original electrónico. Dicha copia será considerada copia auténtica por el hecho de incorporar un código seguro de verificación que permita cotejarla con el documento electrónico original. El cotejo en sí no es requisito para la validez del documento en papel, sino el simple hecho de que se pueda realizar.

8.2 Uso de la impresión segura en el Ayuntamiento de Pamplona

Los mecanismos de impresión segura se prevén con el objeto de ofrecer un servicio al ciudadano. Por tanto, tiene sentido incorporarlos en aquellos documentos que el ciudadano puede necesitar utilizar en soporte papel.

Para evitar la sobrecarga de los sistemas de verificación a medida que se extienda el uso del documento electrónico, el Ayuntamiento ha previsto la distinción entre los siguientes casos:

- **Documentos destinados exclusivamente a la comunicación con el ciudadano:** Determinados documentos se emiten con la finalidad exclusiva de servir al ciudadano para acreditar ante terceros algún dato de su relación con el Ayuntamiento, o para comunicarle o notificarle la manera como le afectan las actuaciones municipales. Es el caso, por ejemplo, de:
 - Volantes de empadronamiento
 - Recibos del registro de entrada de documentos
 - Oficios de notificación o comunicación

Estos documentos incorporarán siempre, desde su generación, el Código Seguro de Verificación, y serán incorporados a los sistemas de verificación como se describe en los apartados siguientes.

- **Copias de documentos administrativos, obtenidas a través de la carpeta ciudadana:** Los documentos que no están incluidos en la clasificación anterior se emitirán en soporte electrónico para su incorporación a los expedientes administrativos del Ayuntamiento, sin incluir un Código Seguro de Verificación. Sin embargo, los ciudadanos, a través del acceso a los documentos que puedan tener a través de la sede electrónica, la carpeta ciudadana u otros mecanismos de interacción, pueden necesitar de la emisión de una copia auténtica en papel del documento.

Para ello, los entornos de interacción con el ciudadano que permitan la consulta de documentos administrativos incluirán la posibilidad de generar copias auténticas en soporte papel, mediante un botón identificado con un texto como “*Preparar para Impresión segura*” o similar.

Cuando los ciudadanos utilicen esta opción, se generará una copia auténtica del documento firmada con un sello de órgano del Ayuntamiento, que incorporará el código seguro de verificación así como la información sobre el periodo de validez de la copia y el procedimiento para su validación, que el ciudadano podrá imprimir o guardar en soporte electrónico.

- **Copias de documentos administrativos, obtenidas a través de los servicios de atención al ciudadano:** Existe la posibilidad de que el ciudadano que necesita la copia del documento no acceda a los sistemas de tramitación electrónica del Ayuntamiento, sino que se dirija a una oficina de atención al ciudadano. Los trabajadores públicos que presten servicio al ciudadano podrán acceder a la documentación por un canal similar al previsto en el caso anterior, para generar la copia auténtica en papel de la misma manera e imprimirla en interés del ciudadano.

8.3 Procedimiento de generación

8.3.1 Código Seguro de Verificación

El código seguro de verificación será una secuencia de letras y números generada de manera pseudoaleatoria y asociada unívocamente al documento. El sistema de generación deberá garantizar que:

- A través del CSV no se puede obtener información sobre el contenido del documento. Así, por ejemplo, los datos del interesado, el tipo de procedimiento o la fecha de generación no formarán parte visible del CSV.
- Dos documentos distintos no pueden tener un mismo CSV. Para garantizar esto se podrá implementar un simple control de colisiones en el momento de la generación.

8.3.2 Documentos con CSV de origen

Cómo se ha descrito en el apartado 8.2, determinados documentos incorporan un CSV desde su creación, porque se crean con la principal finalidad de ser entregados al ciudadano. Estos documentos serán firmados electrónicamente por el mecanismo que corresponda según el procedimiento de que se trate y atendiendo al modelo de firma electrónica contenido en el capítulo 11 de este PDDE:

- Sello de órgano, en el caso de documentos generados por sistemas de actuación administrativa automatizada
- Firma electrónica del personal al servicio del Ayuntamiento, cuando no aplica su generación automática.

El documento que se pondrá a disposición de los usuarios en servicio de cotejo o validación de CSV será en este caso el mismo que se incorpore al expediente administrativo.

Se contempla expresamente la posibilidad de incluir, en este tipo de documentos, una fecha de caducidad para la posibilidad de verificación o cotejo del CSV, con un contenido como el siguiente:

Este documento podrá ser verificado en la sede electrónica del Ayuntamiento de Pamplona hasta el día dd/mm/aaaa. A partir de dicha fecha, se podrá solicitar al Ayuntamiento una nueva copia a través de la carpeta ciudadana que se encuentra en la misma sede o los servicios de atención ciudadana, mediante los datos de identificación del expediente.

Esta posibilidad no está en uso actualmente, pero en un futuro el volumen de documentación sujeta a cotejo puede obligar a hacer uso de la misma. En este caso, será necesario decretar la caducidad de los documentos emitidos con CSV y sin fecha de caducidad en el pasado, y darle a dicha decisión la publicidad necesaria.

8.3.3 Generación de copias auténticas

En el caso de los documentos que no incorporen el CSV en el momento de su creación, se prevé la posibilidad de generar copias auténticas para su impresión a solicitud del interesado. Cuando se soliciten tales copias, el sistema informático cumplirá automáticamente los siguientes pasos:

- a. Generar una copia del contenido íntegro del documento, en formato PDF.
- b. Añadir al pie de cada página del documento, o ubicación alternativa que no interfiera en su contenido, el Código Seguro de Verificación (CSV), generado como se ha indicado previamente.
- c. Añadir al pie de cada página del documento la información sobre el procedimiento de validación, incluida la URL del servicio de verificación del CSV dentro de la Sede electrónica.

- d. Añadir al pie de cada página la mención: “*Copia auténtica en soporte papel de un documento original electrónico, emitida el dd/mm/aaaa en n páginas. Caduca a los n meses*”. Alternativamente, se podrá incluir la indicación “*Vigencia indefinida*”.
- e. Este documento PDF será firmado electrónicamente mediante un sello de órgano de la Secretaria General del Ayuntamiento. La firma incorporará un sello de tiempo.
- f. El documento copia se almacenará en el repositorio específico de copias auténticas, que será accesible desde la sede electrónica del Ayuntamiento.

En caso de que se haya emitido anteriormente una copia auténtica del mismo documento, el sistema presentará al interesado dicha copia auténtica en lugar de generar una nueva, a menos que el período de vigencia restante para esa copia sea inferior a 6 meses.

8.4 Procedimiento de validación

Para el cotejo de los documentos, los interesados se dirigirán a la Sede Electrónica del Ayuntamiento, donde se puede acceder al servicio de **Comprobación de documentos electrónicos mediante Código Seguro de Verificación**. En dicho servicio se debe introducir íntegramente el CSV que consta en el documento que se coteja. Si el CSV coincide con un documento disponible para su consulta, el sistema retorna:

- En el caso de documentos generados originalmente con código CSV, el documento original.
- En el caso de copias auténticas, el documento copia, firmado con el sello electrónico que garantiza la validez de la copia.

8.4.1 Caducidad de la opción de comprobación

Se ha previsto que, en el momento de la generación de los documentos destinados a impresión segura, estos incorporen una fecha a partir de la cual no será posible su comprobación. Esto se hace teniendo en cuenta:

- Que posibles cambios tecnológicos en el futuro puedan hacer imposible o demasiado compleja acceder a cualquier documento generado con anterioridad de manera automática desde la sede electrónica.
- Que determinados expedientes pueden estar sujetos incluso a procedimientos de eliminación, en cuyo caso el Ayuntamiento estaría obligado en todo caso a eliminar la documentación de origen.
- Que los ciudadanos siempre tienen la opción de solicitar al Ayuntamiento la emisión de una nueva copia, incluso de documentos pertenecientes a expedientes cerrados,

de acuerdo con lo que establece el artículo 6.2.e) de la Ley 11/2007 y, a partir del 2 de octubre de 2016, el artículo 27.4 de la Ley 39/2015.

El hecho de que se alcance la fecha límite de comprobación de un documento no obliga al Ayuntamiento a hacerlo inaccesible, pero permite que no se tengan que hacer esfuerzos adicionales para mantenerlo disponible. Cuando los condicionantes tecnológicos lo requieran, todos los documentos cuyo periodo de comprobación haya finalizado podrán ser retirados del sistema de comprobación.

En todo caso, los CSV de documentos retirados del sistema deberán conservarse, asociados al dato de que el documento caducó, para evitar la reutilización de dichos códigos y posibles colisiones en el futuro.

8.5 Custodia de los elementos de verificación

Para recuperar el documento, el sistema de validación puede trabajar con dos estrategias:

- Acceder directamente a la base de datos de documentos del Ayuntamiento.
- Disponer de una base de datos separada, en la que se encuentre únicamente la información sobre los documentos sujetos a cotejo. Esta alternativa no es necesaria actualmente, pero se prevé en atención a la posibilidad de que en el futuro los documentos sujetos a cotejo se puedan encontrar en diferentes entornos (expedientes cerrados o incluso trasladados al archivo definitivo), en cuyo caso será más eficaz que los documentos sujetos a cotejo se guarden en una única base de datos con esta finalidad y se eliminen transcurrido su periodo de validez.

En cualquier caso, hay que tener en cuenta que:

- o En el caso de documentos generados originalmente con CSV, el documento original se incorporará a un expediente administrativo y se le aplicarán los criterios de disposición o preservación que correspondan. En el entorno de consulta se almacenará una copia que podrá ser eliminada tan pronto como deje de ser útil.
- o En el caso de copias auténticas generadas automáticamente para su impresión segura, la copia podrá ser eliminada tan pronto como deje ser útil, ya que el documento que forma parte del expediente es el documento original del cual se extrajo copia.

No es necesario, por tanto, prever procedimientos específicos para la preservación de los documentos generados con fines de impresión segura.

En cuanto a los permisos de acceso, los documentos de impresión segura solo serán accesibles a través de los sistemas de comprobación del CSV, a excepción del acceso que puedan realizar los responsables de gestión documental del Ayuntamiento en el ejercicio de sus competencias.

8.6 Habilitación jurídica

El Ayuntamiento dará cobertura legal al procedimiento de impresión segura mediante la aprobación del Plan Director del Documento Electrónico.

9. Modelo de preservación

La documentación electrónica requiere, para garantizar su inteligibilidad e integridad a largo plazo, de actuaciones proactivas que permitan preservar el formato del documento y la longevidad de los elementos de seguridad, como firmas electrónicas o sellos de tiempo. Se propondrá una estrategia completa que permita superar estas dificultades.

En este capítulo se hará una descripción de los principios básicos de la preservación digital desde un punto de vista genérico. También, se enumerarán los retos que surgen en el momento de plantearse el garantizar la preservación de la documentación a largo plazo.

A partir de aquí, se definirá un plan de preservación a seguir por la organización, que abarcará todas las fases del ciclo de vida y se establecerán los mecanismos que se emplearán para poder garantizar la preservación de la documentación electrónica. Los principales motivos que llevan al Ayuntamiento a la elaboración de dicho plan son la fragilidad del soporte, la conservación de la validez jurídica de los documentos, la obsolescencia del hardware y software y la obsolescencia del formato.

Este Plan de preservación incluye:

- Definición de la estrategia.
- Formatos de preservación.
- Soluciones tecnológicas.
- Tipo de integración de la solución tecnológica con la herramienta de gestión documental y archivo.
- Identificación de las circunstancias en que las actividades de migración se llevarán a cabo y de los métodos y los fundamentos para realizarlas.
- Controles de calidad de los procedimientos, y de los documentos almacenados.
- Descripción de las responsabilidades de los actores que intervienen en la gestión de la preservación de los documentos y expedientes electrónicos.

9.1 Definición de la estrategia de preservación de los documentos y expedientes electrónicos

El sistema de preservación de documentos electrónicos se encargará de controlar de forma periódica los documentos electrónicos para garantizar la accesibilidad a éstos, el poderlos recuperar y garantizar su validez jurídica.

Este proceso de comprobación periódica chequeará los siguientes aspectos de la documentación electrónica conservada:

- Accesibilidad a soportes
- Capacidad de lectura de formatos
- Validez jurídica de las firmas electrónicas.
- Integridad de los documentos.
- Integridad de los expedientes.

El Ayuntamiento debe aplicar como estrategia de preservación de los documentos y expedientes electrónicos y otros objetos digitales la MIGRACIÓN frente a otras técnicas como la emulación, la preservación de la tecnología, la encapsulación,

Dicha decisión se sustenta en el artículo 6, en concreto el punto 5 de 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, que indica: *La Administración podrá reconvertir, utilizando medios técnicos, el formato de un documento que haya recibido, cuando lo considere necesario para su lectura, almacenamiento y archivo, sin que pueda alterarse el contenido sustantivo del documento.*

Asimismo, tenemos varios estándares internacionales que definen este proceso: ISO 18492 (2008), el propio modelo OAIS con la ISO 14721 (2003) u otros.

El proceso de Migración se realizará de forma automatizada, mediante procedimiento administrativo automatizado y los documentos migrados se garantizarán que son copias auténticas a partir de la firma de éstos con un sello de órgano a nombre del Archivo.

Los procesos de Migración los ejecutará el Archivo, a partir de las resoluciones que tome la Comisión Técnica de Gestión Documental.

Control de formatos: normalización y migración

Las herramientas que permiten la preservación de los documentos en base a la estrategia de Migración requieren de una relación limitada de formatos para poder garantizar en todo momento esta posibilidad de migración.

El Ayuntamiento define en el apartado siguiente los formatos de conservación.

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. En el momento en que se requiera informar del metadato correspondiente se podrán utilizar herramientas de este tipo para detectar el formato de un documento.

9.2 Selección de formato de conservación

9.2.1 Formato de documento de texto o texto que incluyen imágenes:

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

El Ayuntamiento creará los documentos a ser posible en formato PDF/A. En el caso de que los documentos provengan de una tercera fuente, sea un ciudadano u otra administración, se propone su conversión a PDF.

Se propone este formato puesto que es un estándar con una ISO definida, la ISO 19005 (2008) Formato de archivo PDF/A-1, pensado precisamente para garantizar su preservación a lo largo del tiempo.

En el caso de facturas electrónicas el formato a preservar será XML. En este caso la decisión viene motivada por un estándar de factura electrónica el Factura-e, que es en formato XML.

9.2.2 Formatos audiovisuales:

Para imágenes los formatos a preservar serán (entre paréntesis las extensiones):

- Gif (.gif)
- Jpeg (.jpeg, .jpg, .JPE, .spf)
- Tiff (.tiff, .tif, .DNG)

Los formatos de video a preservar serán contenedores MPEG-4. Se propone este formato puesto que está definida en un estándar con una ISO, la ISO/IEC 14496. Asimismo, este formato está contemplado como migrable en las plataformas de archivo electrónico contempladas en este modelo y que permiten la migración.

9.2.3 Otros formatos:

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

El archivo electrónico 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).

9.2.4 Formatos de firma electrónica

Para garantizar la validez jurídica de las firmas electrónicas se aplica el criterio de completar las firmas electrónicas existentes a formatos preservables: XAdES-A, CAdES-A o PAdES-LTV.

Estos tipos de firma están definidos en distintos estándares internacionales como ETSI TS 101 903 XAdES, ETSI TS 102 778 PAdES, ETSI TS 101 733 Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES).

A partir de estas firmas y en el momento en que el sello electrónico caduque, se procederá al resellado de las firmas electrónicas, con un nuevo sello, con una caducidad suficiente y con unos algoritmos de firma actualizados.

9.2.5 Formatos de foliado de expediente

En el caso de foliado el formato a preservar será XML. En este caso la decisión viene motivada por el hecho de que los formatos XML son los que permiten mejor la actuación administrativa automatizada que se aplicaría en el momento de garantizar la integridad del expediente electrónico.

9.2.6 Conservación de bases de datos

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

Aunque cabría la posibilidad de archivar en el archivo electrónico, mediante fotos fijas en el tiempo de los valores 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 (modelo de datos, modelo lógico y físico, diagramas entidad-relación...).

Dada la complejidad de la conservación de las bases de datos en el estado actual de la técnica, se valorará la generación y custodia de los listados necesarios en formato PDF/A.

9.3 Requerimientos de los elementos a transferir.

Para poder transferir un expediente electrónico a la plataforma de archivo electrónico se deberán cumplir los siguientes requerimientos:

1. Los expedientes deben estar en ALMADOC
2. Los expedientes deben estar cerrados.
3. Los expedientes deben estar foliados. El foliado debe ser íntegro con los documentos que forman parte de éste y con los resúmenes criptográficos de éstos.
4. Los metadatos obligatorios de los documentos, expedientes y firmas deben estar correctamente informados.
5. Los documentos deben tener un formato reconocido, gestionable y no obsoleto por parte de la plataforma de archivo electrónico.
6. Las firmas electrónicas de los documentos y expedientes electrónicos deben estar completadas a un formato preservable.

9.4 Identificación de las circunstancias en que las actividades de migración se llevarán a cabo y de los métodos y los fundamentos para realizarlas.

Para proceder a ejecutar un proceso de migración, la Comisión Técnica de Gestión Documental habrá tenido que dictaminar qué formatos son obsoletos y a qué formato se deben migrar.

9.4.1 Proceso de conversión de formatos obsoletos

La herramienta de archivo electrónico ofrecerá un servicio que permita 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:

9.4.1.1 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 convertidos.

9.4.1.2 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.

9.4.1.3 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.

9.4.1.4 Autenticación de copia:

Para avalar la autenticidad de la copia resultante del proceso, sobre los documentos convertidos se aplicará una firma electrónica.

9.4.1.5 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, y comprobaciones.

La información que debe recogerse es la siguiente:

- documentación de acciones realizadas 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, y
- los ficheros afectados por la conversión.

9.4.2 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 nunca deben superar los periodos recomendados por los fabricantes de los dispositivos.

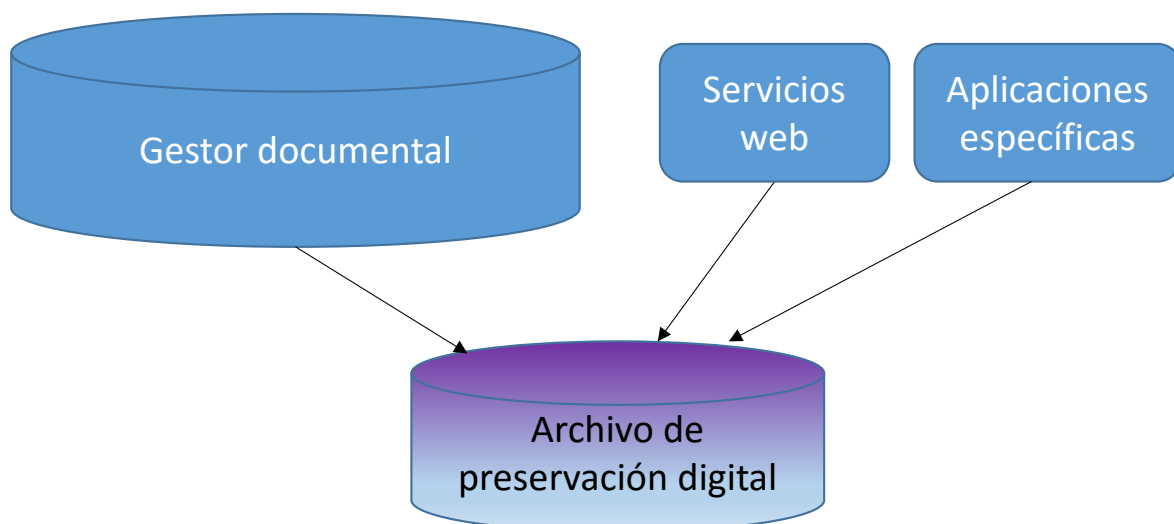
Si se determina que el soporte de almacenamiento utilizado para la custodia ya no es el apropiado, debe establecerse una migración de soportes. La migración difiere del refresco en que los documentos electrónicos son reescritos en un soporte diferente al inicial.

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.

9.5 Soluciones tecnológicas

El Archivo debe garantizar la preservación a largo plazo de los recursos digitales, teniendo en cuenta que, en relación con la documentación digital, la simple conservación de los soportes no implica la adecuada accesibilidad, legibilidad o integridad de la información en el futuro.

Partiendo de la situación actual y de las soluciones actuales en este ámbito, proponemos la siguiente arquitectura para la preservación digital:



La solución de preservación digital debe contemplar los siguientes elementos:

1. Plataforma de preservación digital. Sería la herramienta que permita gestionar los objetos digitales a lo largo del tiempo. Esta plataforma deberá permitir la recepción

de los objetos digitales, y en función del tipo validar su integridad y autenticidad tras ser admitidos para su preservación. Una vez entrados los objetos la plataforma deberá garantizar el acceso, en cualquier momento, para las personas autorizadas. La herramienta también permitirá ejecutar procesos de migración de formatos para garantizar su accesibilidad a lo largo del tiempo. Más adelante se entrará con más detalle en sus funcionalidades.

2. Conjunto de servicios que permiten enviar los objetos digitales en la plataforma desde diferentes fuentes: gestores documentales – ALMADOC (para la gestión de documentos, expedientes, metadatos y firmas electrónicas), aplicaciones específicas o incluso Web Services para que eventualmente y de forma externa se puedan enviar expedientes electrónicos con sus documentos a la plataforma de preservación digital.

9.5.1 Garantías a cubrir en la preservación de objetos digitales

La plataforma deberá garantizar para cada objeto digital:

1. Que el objeto sea localizable y recuperable. Este es el primer elemento clave en una plataforma de preservación de objetos digitales. Aunque esta función ya la cubren la mayoría de herramientas de almacenamiento de objetos digitales, es necesario que la solución sea una solución en red, mantenida por los servicios informáticos y en servidores de éste. Por ejemplo, una solución basada en CD-Roms o DVD no sería válida debido a que en el tiempo estos sistemas no serán accesibles y lo más seguro es que nadie se preocupará de ir ejecutando la sustitución de soportes.
2. Que el objeto sea, una vez localizado y recuperado, interpretable. Es decir, que para el documento que se ha recuperado, exista el software adecuado para poder gestionar, visualizar y verificar su integridad. Para garantizar esto en el tiempo habrá que aplicar alguna de las estrategias de preservación que se explicarán a continuación.
3. Que el objeto una vez localizado, recuperado e interpretado se pueda garantizar que sea idéntico al original, tanto a nivel de contenidos como de validez jurídica (en su caso). Hay que garantizar pues el concepto de autenticidad. Para garantizarlo, hay que asegurar que el objeto que entró era el original, que se ha mantenido en el tiempo de forma sin alteraciones y que hoy podemos probar que esto ha sido así.

9.5.2 Requerimientos funcionales de la plataforma de preservación digital

La plataforma de archivo electrónico cumplirá la ISO 14721: 2003 (OAIS) y en base a ello cumple los siguientes requerimientos funcionales:

NOTA: **(O)** significa que es un requerimiento Obligatorio a cumplir por la plataforma y **(R)** identifica que es un requerimiento Recomendable que cumpla la plataforma.

1. Repositorio de custodia de objetos digitales. La plataforma deberá disponer de un repositorio que pueda almacenar los diferentes objetos digitales que pueda recibir por parte de las fuentes externas. Este repositorio debe poder guardar los objetos en diferentes dispositivos físicos y diferentes servidores, permitiendo el crecimiento de forma ilimitada (en función de los recursos de almacenamiento de que disponga el Ayuntamiento). Los objetos y metadatos se podrán guardar en bases de datos o en plataformas de gestión documental o repositorios tipo Fedora.
 - a. El software debe permitir el crecimiento de la capacidad de almacenamiento de los objetos de forma ilimitada (O)
 - b. El repositorio debe permitir guardar objetos tanto individuales como en paquetes (tipo expedientes) (O)
 - c. El repositorio debe permitir acceder a los objetos de forma unitaria (O)
 - d. El repositorio debe ser independiente de la tecnología donde se guarden físicamente los objetos (Servidores y Disco) (O)
 - e. Debe permitir crear diferentes Fondos Documentales donde guardar los objetos (O)
 - f. Cada Fondo Documental tiene que tener su propio Cuadro de Clasificación (O)
 - g. Cada Fondo Documental tiene que tener su propio Calendario de Retención (O)
 - h. Cada Fondo Documental puede tener políticas de acceso diferentes (O)
2. La plataforma deberá disponer de unos servicios de adquisición de objetos digitales. Dentro de estos servicios habrá tanto la opción vía web de carga del objeto, información de los metadatos del objeto, preparación del objeto para su preservación: creación del paquete de archivo, envío del objeto al repositorio y regreso del comprobante de recepción del objeto por parte del repositorio. Este comprobante contendrá siempre un código único de número de depósito que servirá para futuras recuperaciones. Asimismo, habrá un conjunto de Web Services para poder hacer la recepción del objeto digital, la validación del objeto digital, la generación del paquete de archivo, la generación de información de descripción de paquete de archivo, el retorno del comprobante de entrega del objeto.
 - a. El sistema debe permitir el ingreso de objetos a partir de la carga manual a través de un entorno Web, que permita subir el objeto, entrar los metadatos y hacer la propuesta de ingreso. (R)
 - b. El sistema debe permitir el ingreso de objetos a partir de Web Services. (O)

- c. El sistema debe permitir el ingreso de objetos de forma asíncrona, de tal forma que se pueda hacer el envío de una gran cantidad de objetos y por la noche, por ejemplo, ir haciendo los procesos de ingreso. (O)
- d. El sistema de ingreso debe comprobar la integridad de los objetos introducidos (O)
- e. El sistema de ingreso debe poder generar el índice de los objetos compuestos enviados (R)
- f. El sistema de ingreso debe comprobar los formatos de los objetos enviado (O)
- g. Los formatos que la plataforma debe permitir recepcionar deben ser: PDF, PDF / A, XML, MPG4 (O)
- h. Los formatos posibles a recepcionar deben ser: Microsoft Office y Open Office, etc. (R)
- i. El sistema de ingreso debe validar las firmas electrónicas de los objetos introducidos (O)
- j. Las firmas electrónicas que la plataforma debe aceptar serán XAdES-C, XAdES-A, CAdES-C, CAdES-A, PAdES-C, PAdES-LTV (O)
- k. Las firmas electrónicas que la plataforma debe aceptar serán XAdES-BES, XAdES-T, etc. (R)
- l. El sistema debe poder completar las firmas que no sean -A o LTV a este formato preservable (R)
- m. El sistema debe incorporar a las firmas electrónicas preservables un sello de tiempo (O)
- n. El sistema debe comprobar que los metadatos obligatorios están correctamente informados antes de ejecutar el ingreso del objeto (O)
- o. El sistema debe permitir definir los metadatos obligatorios a estar informados para cada objeto a ingresar, así como los optativos (R)
- p. El sistema debe convertir los paquetes de entrada en paquetes de archivo para su conservación (O)
- q. El sistema debe tener un registro de entradas que sea íntegro e inalterable, y disponer de una consulta (O)
- r. El sistema debe tener una herramienta de explotación del registro (R)
- s. El sistema debe poder emitir recibos de las ingestas. Estos recibos deben ser XML y estar firmados en formato XAdES-A (O)
- t. El sistema acepta objetos cifrados (R)

3. La plataforma deberá disponer de un servicio de gestión de objetos digitales. Esta plataforma dispondrá de un entorno web que permitirá al administrador de la plataforma poder gestionar los objetos digitales introducidos en el repositorio. Esta herramienta debe permitir crear y gestionar repositorios y jerarquías de almacenamiento, gestionar las normas y estrategias de preservación, debe permitir definir los planes de migración, debe permitirles ejecutar, total o parcialmente, debe permitir verificar los procesos de migración y debe generar las evidencias necesarias para poder auditar los procesos de migración. Asimismo, debe permitir procesos de eliminación en base a políticas de conservación que se informarán en la plataforma.
 - a. El sistema de gestión de la plataforma debe permitir:
 - i. Interfaz de usuario de administrador (O)
 - ii. Crear Fondo Documental (O)
 - iii. Crear y mantener Cuadros de Clasificación para cada Fondo Documental (O)
 - iv. Importar Cuadros de Clasificación de otros entornos (R)
 - v. Crear y mantener Calendarios de retención para cada Fondo Documental (O)
 - vi. Importar Calendario de retención de otros entornos (R)
 - vii. Gestionar los usuarios y plataformas que pueden hacer ingreso de objetos (O)
 - viii. Gestionar los usuarios y plataformas que pueden hacer consultas de objetos (O)
 - ix. Gestionar Roles (R)
 - x. Conectarse con directorios de usuarios para gestionar estos usuarios (R)
 - xi. Programación de procesos de eliminación de objetos electrónicos (O)
 - b. El sistema de gestión de la plataforma debe permitir en cuanto a la integridad de los objetos digitales:
 - i. Extensión de la validez criptográfica de los objetos digitales con firma electrónica (O)
 - ii. Verificación continua de la validez criptográfica de los objetos digitales con firma electrónica (O)
 - iii. Verificación continua de la integridad de todos los objetos digitales preservados (O)

- c. El sistema debe permitir en cuanto a la migración de formatos:
 - i. Interfaz de usuario para los administradores de la plataforma (O)
 - ii. Mantenimiento de los formatos tecnológicos admitidos para su preservación (O)
 - iii. Mantenimiento de herramientas de migración (O)
 - iv. Programación de planes de migración (O)
 - v. Programación de planes de migración piloto (R)
 - vi. Procesos de comprobación de procesos de migración (O)
4. La plataforma deberá disponer de unos servicios de consulta / recuperación de objetos digitales. Este módulo permitirá, previa identificación de los usuarios (personas o sistemas a través de Web Services) el acceso a los objetos. En cuanto a las personas se podrá interrogar al repositorio en base a los metadatos de los objetos. En cuanto a los Web Services, la interrogación se realizará en base a los números de depósito. Una vez identificado el objeto, la plataforma convertirá el paquete de archivo en un paquete gestionable por quien haya hecho la solicitud. En el caso de Web Services se devolverá un XML que contendrá el objeto y los metadatos asociados. En el caso de consulta vía web, se devolverá el objeto en un formato interpretable por el usuario.
 - a. Dar acceso a usuarios (O)
 - b. Generación de paquetes de consulta (O)
 - c. Interfaz de usuario para la consulta de paquete (O)
 - d. Generación de copias en formato interpretable por el usuario de los objetos (O)
 - e. Generación de copias auténticas de los objetos preservados (R)
 - f. Sistema de consulta múltiple de paquetes (O)
5. La plataforma deberá disponer de unos servicios de gestión de la propia plataforma. Desde este módulo se configurarán permisos, usuarios, accesos, copias de seguridad, auditorías del sistema, acceso a las evidencias de la plataforma entre otros.
 - a. Interfaz de usuario de administración (O)
 - b. Generar copias de seguridad (O)
 - c. Recuperar copias de seguridad (O)
 - d. Generar informes (R)
 - e. Auditoria del sistema (O)

Otros requerimientos:

- a. Debe permitir instalar tres entornos:
 - Entorno de desarrollo (R)
 - Entorno de pre-producción (O)
 - Entorno de producción (O)
- b. Se deberá incluir la siguiente documentación:
 - Descripción de los flujos de proceso de todas las actividades y operaciones del archivo electrónico (R)
 - Documentación de diseño, de acuerdo con la especificación UML. (R)
 - Manuales de configuración, tanto de usuario como de administrador, de todos los servicios del archivo electrónico (O)
 - Manuales detallados de producto (O)
 - Guía para la integración de los servicios en aplicaciones clientes (O)
 - Procedimientos detallados de gestión, operación y seguridad (O)
- c. La empresa debe proporcionar la siguiente formación:
 - Plan de formación para:
 - i. Personal de dirección y altos cargos (R)
 - ii. Personal técnico y de apoyo (O)
 - iii. Personal de Archivo (O)
 - iv. Personal de procedimientos y auditoría (O)
 - Otros que se consideren necesarios para el logro del máximo grado de conocimiento del sistema por el personal del Archivo (R)

9.5.3 Alternativas actuales de preservación de objetos digitales

En estos momentos hay diferentes opciones a la solución de preservación de objetos digitales:

9.5.3.1 iArxiu

El iArxiu es un servicio de preservación y archivo electrónico que garantiza que los expedientes / documentos que genera o recibe una organización en el ejercicio de sus funciones se mantengan íntegros, fiables, auténticos y accesibles a lo largo de su ciclo de vida.

Aunque el Consorcio AOC da el servicio de preservación en base a esta solución, ofrece también la posibilidad a otras administraciones públicas, previo convenio de colaboración, a la cesión del código a cualquier administración pública.

El producto incluye la prestación de unos servicios relacionados con su conservación a largo plazo:

- Servicios de migración de documentos y visualización de documentos
- Servicio de evidencia electrónica relacionado con la preservación de las firmas electrónicas)

Esta es posiblemente la solución más completa de todas las alternativas actuales. La solución iArxiu es un producto desarrollado por el Consorcio AOC: <http://www.aoc.cat/Inici/SERVEIS/Gestio-interna/iArxiu>.

9.5.3.1.1 Funcionalidades contempladas en el producto

La plataforma iArxiu tiene las siguientes funcionalidades:

Ingreso

- Creación de peticiones de transferencia de documentos / expedientes
- Aprobar, rechazar y aceptar las solicitudes de transferencia de documentos / expedientes

Archivo

- Incluye el repositorio digital donde se almacenan y custodian los documentos / expedientes
- Asegura la conservación de los documentos electrónicos aplicando lo previsto en el Esquema Nacional de Seguridad, en cuanto al cumplimiento de los principios básicos y los requisitos mínimos de seguridad, mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en que se almacenen los documentos, de acuerdo con la categorización de los sistemas

Consulta

- Búsqueda básica y avanzada mediante los metadatos de los documentos / expedientes
- Consulta en línea de los documentos
- Expedición de copias auténticas y conversión en línea de los documentos a nuevos formatos
- Descarga del informe de evidencia

Administración

- Gestión de los usuarios de la plataforma

- Gestión de las políticas de acceso a los documentos
- Gestión de las políticas de retención y disposición de los documentos
- Gestión de las series documentales
- Consulta de estadísticas de uso y del registro de acciones

Preservación

- Gestión y ejecución de políticas de migración de documentos, de consistencia y de resellado.
- Gestión de los formatos de los ficheros

9.5.3.1.2 Tipología de solución

La solución iArxiu tiene las siguientes características:

Tipo de solución	Software
Estrategia de preservación	Migración
Cumplimiento OAIS	Si
Formatos aceptados	application / java-archive (jar) application / javascript (j) s application / MSAccess (accdb) application / msword (doc) application / ogg (ogg) application / pdf (pdf) application / pkcs7-mime (p7c) application / pkcs7-signature (p7s) application / postscript (ps, eps, epsf) application / rtf (rtf) application / vnd.ms-access (mdb) application / vnd.ms-excel (xls) application / vnd.ms-outlook (msg) application / vnd.ms-powerpoint (ppt, pps) application / vnd.oasis.opendocument.chart (odc)

<p>application / vnd.oasis.opendocument.database (ODB)</p> <p>application / vnd.oasis.opendocument.formula (ODF)</p> <p>application / vnd.oasis.opendocument.graphics (ODG)</p> <p>application / vnd.oasis.opendocument.image (odio)</p> <p>application / vnd.oasis.opendocument.presentation (ODP)</p> <p>application / vnd.oasis.opendocument.spreadsheet (ods)</p> <p>application / vnd.oasis.opendocument.text (odt)</p> <p>application / vnd.oasis.opendocument.text-master (odm)</p> <p>application / vnd.openxmlformats-officedocument.presentationml.presentation (pptx)</p> <p>application / vnd.openxmlformats-officedocument.presentationml.slide (sldx)</p> <p>application / vnd.openxmlformats-officedocument.presentationml.slideshow (ppsx)</p> <p>application / vnd.openxmlformats-officedocument.spreadsheetml.sheet (xlsx)</p> <p>application / vnd.openxmlformats-officedocument.wordprocessingml.document (docx)</p> <p>application / x-gzip (gz, gzip)</p> <p>application / xhtml + xml (xht, xhtml)</p> <p>application / xml (xsd, xsl)</p> <p>application / x-PKCS12 (p12, PFX)</p> <p>application / x-pkcs7-certificates (p7B)</p> <p>application / x-rar-compressed (raro)</p> <p>application / x-tar (tar)</p> <p>application / x-x509-es-cierto (cer, crt, der)</p> <p>application / zip (zip)</p> <p>audio / mpeg (m3u, mp3)</p> <p>audio / x-aiff (aiff, ayf, AIFC)</p> <p>audio / x-ms-wma (asf, wma)</p> <p>audio / x-wav (wav, wave)</p> <p>image / bmp (bmp, DDB, dib)</p>

	<p>image / gif (gif)</p> <p>image / jpeg (jpeg, jpg, JPE, spf)</p> <p>image / png (png)</p> <p>image / svg + xml (svgz, svg)</p> <p>image / tiff (tiff, tif, DNG)</p> <p>image / vnd.dwg (dwg)</p> <p>image / vnd.dxf (dxf)</p> <p>message / RFC822 (eml)</p> <p>text / css (css)</p> <p>text / html (html, htm, jsp, php)</p> <p>text / plain (txt, tsv, csv, antes, asc)</p> <p>texto / sgml (sgml)</p> <p>text / xml (xml, gml)</p> <p>video / mp4 (mp4)</p> <p>video / mpeg (mpeg, mpg)</p> <p>video / quicktime (mov, qtm)</p> <p>video / x-msvideo (abuelo)</p>
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Si
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	Si

9.5.3.1.3 Estimación de costes de la solución

Para este estudio hemos tenido en cuenta los diferentes proyectos que se han hecho con el Consorcio AOC, donde éste nunca ha cobrado por la licencia, sino sólo por el apoyo a la puesta en marcha y la auditoría de la plataforma, que esté correctamente implantada.

Los costes aproximados podrían ser:

Concepto	Importe
Hardware (50-150 TB)	Entre 60.000 y 100.000, - €
Instalación personalización del software	25.000, - €
Soporte y Auditoría	15.000, - €
TOTAL	100.000, - €

9.5.3.1.4 Contacto

Para más información, se puede contactar a:

Consorcio AOC

C / Tánger, 98

22 @ Edificio Interface

08018 Barcelona

www.aoc.cat

Persona de contacto: Miquel Estapé

info@aoc.cat

Telf. +34 93 272 25 00

9.5.3.2 Archive

La solución Archive es una solución ofrecida por el Ministerio de Hacienda y Administraciones Públicas a las diferentes administraciones públicas españolas a la que se puede añadir cualquier administración pública que esté en el Sistema de archivos español.

Archive es un servicio de preservación y archivo electrónico que garantiza que los expedientes/documentos que genera o recibe una organización en el ejercicio de sus funciones se mantengan íntegros, fiables, auténticos y accesibles a lo largo de su ciclo de vida.

Respecto a su implantación, se puede escoger si se quiere adquirir como producto, instalando en el hardware propio del Ayuntamiento el código fuente disponible en <http://administracionelectronica.gob.es/ctt/archive/descargas#.VyoDzPmLQ2w>, o como un servicio firmando el correspondiente convenio con el Ministerio de Hacienda y Administraciones Públicas.

9.5.3.2.1 Funcionalidades contempladas en el producto

La plataforma Archive tiene las siguientes funcionalidades:

Ingreso

- Creación de peticiones de transferencia de documentos/expedientes.
- Aprobar, rechazar y aceptar las solicitudes de transferencia de documentos/expedientes.
- Permite obtener actas de ingreso.
- Permite la generación y gestión de reglas de validación SIP (Archival Information Package).
- El ingreso se realiza expediente a expediente. Es decir, cada acta de transferencia solo permite incluir un solo expediente.

Archivo

- Asegura la conservación de los documentos electrónicos aplicando lo que prevé el Esquema Nacional de Seguridad, en cuanto al cumplimiento de los principios básicos y de los requisitos mínimos de seguridad, mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.
- Permite la reapertura del expediente a través de un acta de devolución a la oficina que lo gestionaba antes de transferirlo al archivo.
- En breve, permitirá la gestión de expedientes híbridos incluyendo los metadatos de topográfico y localización.

Consulta

- Búsqueda básica y avanzada mediante los metadatos de los documentos/expedientes.
- Consulta en línea de los documentos.
- Expedición de copias auténticas y conversión en línea de los documentos a nuevos formatos.
- Descarga del informe de evidencia.

- Permite la impresión segura y la generación del correspondiente CSV que podrá ser consultado a través de esta herramienta.

Administración

- Gestión de los usuarios de la plataforma.
- Gestión de las políticas de acceso a los documentos.
- Gestión de las políticas de retención y disposición de los documentos permitiendo la Eliminación Permanente, Conservación Permanente y Pendiente de Dictamen.
- No permite la eliminación parcial.
- Gestión de las series documentales.
- Consulta de estadísticas de uso y del registro de acciones.
- Gestión de los metadatos del Esquema de Metadatos de la Norma Técnica de Interoperabilidad a las que se les pueden añadir de personalizadas para cada archivo.
- Permite la gestión del cuadro de clasificación.
- Permite la encriptación de la información.
- Permite la notificación de los cambios de estados de expedientes.

Preservación

- Gestión y ejecución de políticas de migración de documentos, de consistencia y de resellado.
- Gestión de los formatos de los ficheros.
- En breve estarán disponibles de funcionalidades de:
 - Resellado de la documentación.
 - Conversiones masivas de formato.

9.5.3.2.2 Tipología de solución

La solución Archive tiene las siguientes características:

Tipo de solución	Software o servicio
Estrategia de preservación	Migración
Cumplimiento OAIS	Sí
Formatos aceptados	Múltiples formatos
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Sí
Aporta la solución almacenamiento	Sí en modalidad servicio
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, QdC, Calendario de conservación	Sí

9.5.3.2.3 Pros y contras de la solución

Pros:

- ✓ Es un servicio gratuito y por tanto no hay costes ni de inversiones ni de mantenimiento ya que el Ministerio garantiza las inversiones y el mantenimiento de la solución. Sin embargo, no sería extraño que en el futuro hubiese algún coste por información almacenada.
- ✓ La ley prioriza el uso de esta herramienta. Si no se utiliza esta habrá que hacer un informe argumentando porqué, previsiblemente, será por tanto el estándar de solución de archivo electrónico único.
- ✓ Cumple con los requerimientos de la Ley y de los Esquemas Nacionales de Seguridad e Interoperabilidad.
- ✓ Es de código abierto con licencia EUPL (European Public License).
- ✓ En caso de adquirirlo en modalidad de producto, los documentos se guardarán siempre en el Ayuntamiento.
- ✓ En caso de adquirirlo en modalidad de servicio, no hay coste de hardware ni de instalación.

- ✓ En un futuro próximo se debe poder resellar la documentación y realizar conversiones masivas de formatos.
- ✓ Permite incluir metadatos personalizados para cada Archivo.
- ✓ Permite la impresión segura de los documentos que custodia.
- ✓ Permite la reapertura del expediente a través del acta de devolución.
- ✓ En breve, permitirá la gestión de expedientes híbridos.
- ✓ Permite la encriptación de la información.
- ✓ Permite la notificación de los cambios de estado de un expediente.

Contras:

- ✗ En caso de adquirirlo en modalidad de servicio, los documentos no residirán en el ayuntamiento.
- ✗ En caso de adquirirlo en modalidad de producto, hay coste de hardware, de integración.
- ✗ No habrá personalizaciones del servicio, habrá que adaptarse.
- ✗ Hay pocos usuarios actualmente.
- ✗ No hay experiencias de integración.
- ✗ El nivel de servicio, en caso de problemas, se supone que no será el mismo que con una empresa privada.
- ✗ Está en desarrollo. Por tanto, las funcionalidades actuales no son definitivas, sino que se pueden ampliar en un futuro próximo.
- ✗ Actualmente, para poder dar de alta una serie, es obligatorio incluir el código SIA de la serie. Se está valorando utilizar otro tipo de codificación de series ya que en estos momentos está dando problemas.
- ✗ Actualmente, no permite el ingreso masivo de expedientes.
- ✗ Solo se permite incluir un sol expediente a cada acta de transferencia.
- ✗ No permite la eliminación parcial.

9.5.3.2.4 Estimación de costes de la solución

La solución se puede utilizar en modalidad servicio o como producto.

Solo hay que firmar un convenio con el Ministerio de Hacienda y Administraciones Públicas en caso que se quiera adquirir Archive en modalidad de servicio y, por tanto, alojar los expedientes en el MINHAP.

No tiene coste hasta estos momentos.

9.5.3.2.5 Contacto

Para más información, se puede contactar en:

<https://ssweb.seap.minhap.es/ayuda/consulta/archive>

También se puede acceder al siguiente enlace para descargar el código del documento y manuales de usuario:

<http://administracionelectronica.gob.es/ctt/archive/descargas#.VyoDzPmLQ2w>

9.5.3.3 M4-LTA

Esta es una solución comercial distribuida por la empresa IN2.

M4-LTA es una plataforma que permite custodiar objetos documentales que están sujetos a períodos de permanencia establecidos, normalmente, por un marco legislativo.

El producto incluye la prestación de unos servicios relacionados con su conservación a largo plazo:

- Servicio de evidencia electrónica relacionado con la preservación de las firmas electrónicas)

9.5.3.3.1 Funcionalidades contempladas en el producto

La plataforma M4-LTA tiene las siguientes funcionalidades:

- Gestión de múltiples cuadros de clasificación (multi-entidad).
- Gestión de tablas de evaluación simples, que se pueden asociar a espacios documentales concretos de un cuadro de clasificación (en un espacio documental de una entidad).
- Las principales operaciones que se pueden ejecutar desde una tabla de evaluación son:
 - En el ingreso:
 - Transformación de formato (PDF-A).
 - Completado de la firma a nivel de archivo.
 - Copiar en otro repositorio o espacio documental.
 - Configuración del periodo de retención.
 - Cuando corresponda según configuración. ◦ Re-sellado de tiempo de las firmas a nivel de archivo.
 - Copiar en otro repositorio o espacio documental.
 - Mover a otro repositorio o espacio documental.
 - Eliminación segura.

- Creación y custodia de evidencias digitales de cualquier operación que se realice con el repositorio.
- Web Services para la integración con sistemas de la información «clientes» del repositorio: ingreso, investigación, recuperación.
- Aplicación web que permite a usuarios con permisos realizar las operaciones de ingreso, búsqueda y recuperación de los objetos documentales.

9.5.3.3.2 Tipología de solución

La solución M4-LTA tiene las siguientes características:

Tipo de solución	Software o servicio
Estrategia de preservación	No tiene esta funcionalidad
Cumplimiento OAIS	Si
Formatos aceptados	Cualquier documental, que se pueda pasar a PDF
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Si
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	Si

9.5.3.3.3 Estimación de costes de la solución

Los costes aproximados serían:

Concepto	Importe
----------	---------

Hardware (50-150 TB)	Entre 60.000 y 100.000, - €
Software	95.000, - €
Instalación y personalización del software	45.000, - €
TOTAL	200.000, - €

9.5.3.3.4 Contacto

Para más información, se puede contactar a:

IN2

Travessera de Gràcia, 73-79, Ático

08006 Barcelona

www.in2.es

contacto@in2.es

Telf. + 34 902 88 17 76

9.5.3.4 Eversuitecompliance SE

Esta es una solución de software suministrado por la empresa francesa EVER TEAM

Eversuitecompliance es una solución que cumple diferentes estándares de preservación, que permite la preservación a largo plazo de objetos digitales, especialmente documentos.

Funciona integradamente con SharePoint de Microsoft.

El producto incluye también la posibilidad de poder guardar rastro de documentos físicos en su localización física.

9.5.3.4.1 Funcionalidades contempladas en el producto

La herramienta Eversuitecompliance SE tiene las siguientes funcionalidades:

- Es una solución de archivo que permite gestionar en una única aplicación, tanto archivos electrónicos como registros físicos.
- Dispone de un sistema de búsqueda muy potente que permite buscar los diferentes objetos de forma muy rápida. Permite realizar consultas desde SharePoint y SQL Server.
- Guarda trazabilidad de todo el ciclo de vida del objeto dentro en plataforma. Esto permitirá dar una validez legal importante, si el objeto original era auténtico.

- Auditoría: permite a un auditor verificar la conformidad y anticipar los cambios necesarios para hacer frente a los posibles problemas de obsolescencia.
- Dispone de un Cuadro de clasificación y de calendarios de conservación.
- Permite aplicar procesos de eliminación o de conservación permanente.
- Dispone de herramientas de firma electrónica y permite conectarse a servicios de terceros de confianza: sellado de tiempo.
- Herramientas de Migración de los archivos electrónicos, mediante formatos o soportes a largo plazo.
- Implementación de una caja fuerte electrónica.
- Dispone de una gestión de usuarios y políticas de acceso.

9.5.3.4.2 Tipología de solución

La solución EversuiteCompliance SE tiene las siguientes características:

Tipo de solución	Software
Estrategia de preservación	Estandarización de formatos y Migración
Cumplimiento OAIS	Si
Formatos aceptados	La mayoría de formatos.
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Sí, siempre y cuando se pueda pasar a un formato preservable inicialmente.
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	Si

9.5.3.4.3 Estimación de costes de la solución

No disponible.

9.5.3.4.4 Contacto

Para más información, se puede contactar a:

EVER TEAM

336 rue Saint-Honoré

75001 Paris

FRANCE

www.ever-team.com

info@ever-team.com

Telf. +33 (0) 1 72 71 33 00

9.5.3.5 STS PEA

Esta es una solución de software suministrado por la empresa Cecurity

STS PEA es una solución de archivo electrónico que permite la gestión de grandes volúmenes de objetos.

La empresa Cecurity también ofrece la posibilidad del servicio SaaS de archivo electrónico.

9.5.3.5.1 Funcionalidades contempladas en el producto

La herramienta STS PEA tiene las siguientes funcionalidades:

- Plataforma de archivo electrónico de objetos.
- Conversión de los objetos en paquetes de objetos de preservación.
- Mecanismo de consulta para metadatos de los objetos.
- Guarda trazabilidad de todo el ciclo de vida del objeto dentro en plataforma. Esto permitirá dar una validez legal importante, si el objeto original era auténtico. Las evidencias que se guardan están firmadas y disponen de sello de tiempo.
- Auditoría: permite a un auditor verificar la conformidad y anticipar los cambios necesarios para hacer frente a los posibles problemas de obsolescencia.
- Dispone de un Cuadro de clasificación y de calendarios de conservación.
- Permite aplicar procesos de eliminación o de conservación permanente.

- Dispone de herramientas de firma electrónica y permite conectarse a servicios de terceros de confianza: sellado de tiempo.
- Herramientas de Migración de los archivos electrónicos, mediante formatos o soportes a largo plazo.
- Gestión de usuarios y permisos.
- Permite integrarse con la mayoría de sistemas de almacenamiento de alta seguridad: EMC Centera, IBM TivoliStorage Manager, Net AppSnapLock, Hitachi Content platform, ...

9.5.3.5.2 Tipología de solución

La solución STS PEA tiene las siguientes características:

Tipo de solución	Software
Estrategia de preservación	No
Cumplimiento OAIS	Si
Formatos aceptados	La mayoría
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Si.
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	Si

9.5.3.5.3 Estimación de costes de la solución

Modalidad servicio.

El servicio es ofrecido por una subsidiaria de Cecuritygroup, Cecurity Services. Se utilizan las mismas tecnologías, pero en modalidad SaaS.

La empresa garantiza, como tercero de confianza, a sus clientes, el almacenamiento de sus objetos digitales garantizando su integridad, preservación, confidencialidad y trazabilidad de todas las acciones que se han hecho sobre los objetos.

El precio varía en función de los volúmenes. Esta es una primera estimación de costes:

Docs Anuales	Alta Servicio	Mant Servicio Anual
10.000	€ 1.000,00	€ 150,00
25.000	€ 1.500,00	€ 225,00
50.000	€ 2.000,00	€ 300,00
100.000	€ 2.500,00	€ 375,00
250.000	€ 3.000,00	€ 450,00

Producto

El coste aproximado sería:

Concepto	Importe
Hardware (50-150 TB)	Entre 60.000 y 100.000, - €
Software	120.000, - €
Instalación y personalización del software	25.000, - €
TOTAL	205.000, - €

9.5.3.5.4 Contacto

Para más información, se puede contactar a:

SECURITY

75 rue Saint-Lazare

75009 PARIS

www.cecurity.com

<http://www.cecurity.com/en/contact>

Telf. +33 1 56 43 37 37

9.5.3.6 Baratz

La empresa Baratz está desarrollando una solución de preservación de objetos digitales que estará disponible a finales de año.

El desarrollo lo está haciendo con el Ayuntamiento de Terrassa.

Baratz es una empresa especializada en software de gestión de archivos físicos y en estos momentos está desarrollando una plataforma para el archivo electrónico.

9.5.3.6.1 Funcionalidades contempladas en el producto

La herramienta de Baratz tendrá las siguientes funcionalidades a finales de año:

Ingreso

- Inserción de los objetos digitales con control de validación de la estructura.
- Inserción masiva de objetos digitales, con control de validación de la estructura.
- Emisión del recibo de la inserción del objeto digital al repositorio seguro.

Archivo

- Custodia de los objetos digitales.

Consulta

- Búsqueda de los objetos digitales
- Visualización de los objetos digitales.
- Recuperación de los objetos digitales.

Administración

- Gestión de usuarios y definición de perfiles.
- Gestión del cuadro de clasificación. Posibilidad de importar desde un Cuadro de Clasificación del gestor documental.
- Gestión del calendario de preservación.
- Definición del vocabulario de metadatos de los objetos digitales.
- Integración con plataformas de auditoría.
- Exportación del cuadro de clasificación.

Preservación

- Definición de la política de eliminación o disposición.

Otros

- Módulo de integración con directorios LDAP, para el control de acceso.

Para mediados del año 2015 están previstas las siguientes funcionalidades:

Ingreso

- Generación de paquetes Mets.
- Generación del Índice electrónico de expedientes: foliado.

Archivo

- Custodia de los objetos digitales.

Consulta

- Copia certificada de objetos del archivo electrónico.
- Extracción certificada de un Fondo Documental.

Administración

- Mantenimiento de las políticas de resellado.
- Consulta de informes de ejecuciones de migración.
- Consulta de las evidencias de acciones sobre el archivo electrónico. Auditoría.
- Informes de auditoría de las evidencias electrónicas.
- Exportación del calendario de preservación.

Preservación

- Resellado de los objetos.
- Migraciones de formato.
- Herramienta de control de la obsolescencia de los formatos.

9.5.3.6.2 Tipología de solución

La solución de Baratz tendrá las siguientes características:

Tipo de solución	Software
Estrategia de preservación	Migración

Cumplimiento OAIS	Si
Formatos aceptados	Todos los Microsoft office, todos los Open Office, PDF, XML, Zip, Rar, mp3, wav, wma, gif, jpeg, png, tiff, eml, html, texto plano, mp4, mpeg, mov.
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Si
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	Si

9.5.3.6.3 Estimación de costes de la solución

Los costes aproximados serían:

Concepto	Importe
Hardware (50-150 TB)	Entre 60.000 y 100.000, - €
Software	30.000, - €
Instalación y personalización del software	15.000, - €
TOTAL	105.000, - €

9.5.3.6.4 Contacto

Para más información, se puede contactar a:

BARATZ

Raimundo Fernández Villaverde, 28

28003 Madrid

www.baratz.es

informa@baratz.es

Telf +34 91 456 03 60

9.5.3.7 Libsafe

La empresa Libnova ha desarrollado una solución integral de preservación de objetos digitales, que se basa inicialmente en la definición de un plan de preservación que se garantizará en todo el ciclo de vida de los objetos digitales que se preserven.

Dispone además de un sistema adicional para la preservación de grandes volúmenes hasta 1600 Tb para armario rack)

9.5.3.7.1 Funcionalidades contempladas en el producto

Plan de preservación.

- Libsafe dispone de un sistema de documentación interno que permite definir un plan de preservación.
- Es necesario que el material a preservar se adecue a lo que se haya definido en el plan de preservación.

Ingreso

- Inserción de los objetos digitales con control de validación de la estructura definida en el plan de preservación.
- Permite realizar controles de calidad de la imagen a ingresar.
- Permite hacer inserciones en diferentes dispositivos a la vez.
- Guarda evidencia criptográfica de la inserción.
- Hay conversión de la información no estructurada en objetos digitales conservables.

Archivo

- Custodia de los objetos digitales.

Consulta

- Búsqueda de los objetos digitales por valor de metadatos (de origen o generados por la plataforma).
- No hay conversión entre los objetos de archivo y de consulta, pues son los mismos.
- Visualización de los objetos digitales.
- Recuperación de los objetos digitales.

Administración

- Gestión de usuarios y definición de perfiles.
- Permite la auditoría.
- Genera informes automáticos o en el momento en que se le pida.

Preservación

- La plataforma comprueba de forma periódica la integridad de los objetos incorporados. Usar funciones hash MD5 o SHA.
- Alertas en caso de que no se pueda acceder a algún objeto o que éste haya variado.

9.5.3.7.2 Tipología de solución

La solución Libsafe tiene las siguientes características:

Tipo de solución	Software
Estrategia de preservación	No
Cumplimiento OAIS	Si (excepto que los objetos de archivo son igual que los de consulta)
Formatos aceptados	La mayoría de los formatos.
Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	Si
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	No

9.5.3.7.3 Estimación de costes de la solución

Los costes aproximados serían:

Concepto	Importe
Hardware (50-150 TB)	Entre 60.000 y 100.000, - €
Software	25.000, - €
Instalación y personalización del software	15.000, - €
TOTAL	100.000, - €

9.5.3.7.4 Contacto

Para más información, se puede contactar a:

LIBNOVA, SL

Paseo de la Castellana 153

28046 Madrid

www.libnova.com

mcontacto@libnova.es

Telf. +34 91 449 08 94

9.5.3.8 Hardware de almacenamiento con garantía de integridad

Una última posibilidad sería implantar alguna herramienta de algún proveedor de hardware, que aporte una solución de alta disponibilidad e integridad de los datos almacenados.

Estas soluciones sólo garantizan la custodia de los objetos.

9.5.3.8.1 Tipología de solución

Estas soluciones suelen tener las siguientes características:

Tipo de solución	Hardware y software de gestión
Estrategia de preservación	No
Cumplimiento OAIS	No
Formatos aceptados	Todos.

Garantiza la validez jurídica de los documentos a lo largo del tiempo (preservación de firmas)	No
Aporta funcionalidades de gestión del ciclo de vida: eliminación, transferencia, Cuadro de Clasificación, Calendario de conservación	No, se debe hacer desde un Gestor Documental

Existen diferentes empresas que disponen de soluciones en este ámbito:

- EMC con la familia de soluciones centers.
- IBM
- HITACHI
- Hewlett-Packard
- Otros

9.5.3.8.2 Estimación de costes de la solución

Dependen del volumen de datos a almacenar y de los posibles acuerdos que pueda tener el Ayuntamiento con algunos de estos proveedores.

9.5.3.9 CUADRO RESUMEN

Producto: Nombre del producto.

Empresa: Empresa fabricante del producto.

Tipo de Solución: Indica si es un software que se deberá instalar en unos equipos hardware o bien es una solución hardware que lleva un software de gestión específico.

Estrategia de preservación: identifica la estrategia de preservación que incorpora el producto: migración, emulación,

Producto: indica que la empresa suministra un producto que se debe instalar en los equipos del cliente.

Servicio: indica que la empresa suministra un servicio de archivo electrónico, desde la propia empresa, y por lo tanto no es necesario instalar ningún software en los equipos del cliente.

Coste: Valoración aproximada de la solución completa: software + hardware.

Producto	Empresa	Tipo solución	Estrategia de preservación	Producto	Servicio	Coste
iArxiu	Consorti o AOC	Software	Migración	SI	NO	100.000, - €
Archive	MINHAP	Software	Migración	SI	SI	Sin coste por ahora
M4-LTA	IN2	Software	NO	SI	NO	200.000, - €
Eversuitecompliance SE	EVER-TEAM	Software	Migración	SI	NO	-
STS PEA	CECURITY	Software	NO	SI	SI	205.000, - €
Baratz	Baratz	Software	Migración	SI	NO	105.000, - €
Libsafe	Libnova	Software	No	SI	NO	100.000, - €

9.6 Tipo de integración de la solución tecnológica con la herramienta de gestión documental y archivo

El Ayuntamiento dispone en estos momentos de una herramienta de gestión documental, **ALMADOC**.

Dicha herramienta gestiona los metadatos a partir de una base de datos y almacena los documentos en un sistema de ficheros. Dicha herramienta ha sido desarrollada por ANIMSA.

ALMADOC debería:

1. Realizar el foliado de los expedientes. En este proceso se verificaría que los documentos tienen el formato adecuado, las firmas electrónicas son válidas y tienen el formato de firma correcto (si no fuera el caso, se completaría la firma al formato válido de archivo) y se verificaría que los metadatos son correctos.
 - a. En el caso que alguno de estos elementos no fuera correcto o no fuera posible generarlo de forma automática, **no** se procedería a la realización del foliado. En este caso, se procederá a informar al responsable del expediente del hecho y a que tome las medidas oportunas para poder cerrar el expediente. La responsabilidad sobre el expediente continúa en manos del departamento de gestión.
 - b. Solo en el caso en el que se pueda foliar el expediente, es decir que todos los elementos se hayan podido verificar correctamente, se cerraría el expediente y se dejaría pendiente para la transferencia. En el momento en que el Archivo acepta la transferencia, de manera que la responsabilidad sobre el expediente pasa a Archivo.
2. Se debería implementar el proceso de transferencia desde la herramienta ALMADOC que consistiría en generar los paquetes que requiera la herramienta de archivo electrónico y solicitar la transferencia.

A partir de este momento, se pasa el control a la herramienta de archivo que será operada por Archivo y tendrá una bandeja de transferencias pendientes. La herramienta verificará que los paquetes sean correctos: formatos, firmas electrónicas, foliado y metadatos. Y en el caso que sea así, se pasará a la bandeja de objetos a transferir. El operador de Archivo podrá ver estas peticiones y aceptarlas o rechazarlas. En el caso que se acepten, los paquetes se incorporarán al archivo electrónico, se generará un documento electrónico de transferencia, firmado por el Archivo y se mandará al departamento de gestión, el cual deberá conformar la transferencia. En el caso de que no sea aceptada la transferencia, por problemas en los paquetes o porque el Archivo no lo acepta, éste deberá informar del motivo y se comunicará al departamento de gestión. La transferencia no se realizará y se devolverá al estado de pendiente de transferir.

En el caso de que se realice la transferencia podemos tener varios escenarios:

1. **Duplicación de expedientes.** Este escenario consiste en transferir los expedientes, documentos, firmas electrónica y metadatos a la herramienta de archivo, pero manteniéndolos también en ALMADOC. Las consultas de los expedientes por parte del Departamento de Gestión, una vez transferidos se realizará sobre ALMADOC, mientras que las consultas de terceros se harían sobre la herramienta de archivo electrónico. En el momento en que haya una migración de formatos o un proceso de resellado, finalizado éste se realizaría una sustitución de los documentos, expedientes, firmas, y metadatos del ALMADOC, con los que se han actualizado, de forma que la información estaría siempre duplicada. En el caso de que se realicen eliminaciones en el archivo electrónico, se realizarían también en ALMADOC.
2. **Expediente único.** Este escenario consiste en transferir los expedientes, documentos, firmas electrónicas y metadatos a la herramienta de archivo, y al finalizar correctamente este proceso, eliminar los datos, excepto la vinculación con el objeto transferido, de ALMADOC. Las consultas de los expedientes transferidos se realizarían siempre sobre la herramienta archivo electrónico.
3. **Herramienta de migración.** Este escenario consiste en no disponer de una herramienta de archivo electrónico, sino de una herramienta de migración de documentos. En el momento en que sea requerida una migración, ALMADOC, generará los paquetes y los enviará a la herramienta de migración, la cual realizará el proceso y verificará que se ha hecho correctamente. Una vez finalizado se sustituirán los documentos y expedientes migrados en ALMADOC.

Escenario	Pros	Contras
Duplicación de expedientes	<ul style="list-style-type: none"> • Existen herramientas de archivo electrónico que lo permiten. • La integración de ALMADOC al archivo electrónico es sencilla. • El acceso a los expedientes por parte del departamento de gestión es la misma de siempre. • Mayor velocidad de acceso a estos expedientes por parte del departamento de gestión. • Se tiene la información en los dos sitios por lo que se puede recuperar información en caso de problemas. 	<ul style="list-style-type: none"> • La integración del archivo electrónico a ALMADOC es compleja. • Se duplica información. • Si los procesos no están muy bien sincronizados puede haber problemas de integridad entre los expedientes en las dos plataformas.

<p>Expediente único.</p>	<ul style="list-style-type: none"> • Existen herramientas de archivo electrónico que lo permiten. • La integración de ALMADOC a archivo electrónico es sencilla. • No se duplica información. 	<ul style="list-style-type: none"> • El acceso a los expedientes por parte del departamento de gestión es distinto según se hayan transferido o no. • El acceso a los expedientes transferidos por parte del departamento de gestión es más lento. • Se deben implementar sistemas de control de acceso más complejos en la herramienta de archivo.
<p>Herramienta de migración.</p>	<ul style="list-style-type: none"> • La integración con ALMADOC de ALMADOC a herramienta de migración no parece compleja. • El acceso a los expedientes por parte del departamento de gestión es la misma de siempre. • Mayor velocidad de acceso a estos expedientes por parte del departamento de gestión. • No hay problemas de sincronización entre las dos plataformas. • No se duplica información. • La migración a nuevas plataformas será más sencilla que la anterior. 	<ul style="list-style-type: none"> • No existen herramientas de electrónico que lo permiten. • Se deberán implementar muchas funciones sobre ALMADOC, entre las cuales destacamos: calendario de conservación, reglas de eliminación, registro de eliminación, y proceso de resellado. • No se aprovecha tanto el desarrollo ya realizado por empresas especializadas en herramientas de archivo electrónico.

En base a estas posibilidades el Ayuntamiento deberá apostar, en una primera fase, por la Duplicación de expedientes como sistema de integración entre el gestor documental y la plataforma de archivo electrónico. En el momento en que las herramientas de archivo incorporen sistemas de consulta más eficientes, más rápidos y más parecidos a un gestor documental se podrá considerar pasar al segundo modelo, el de expediente único.

9.7 Responsabilidades de los actores intervinientes en la preservación de los Documentos y Expedientes Electrónicos.

En los procesos vinculados a la preservación de los documentos y expedientes electrónicos intervienen los siguientes departamentos, áreas u organismos:

- Archivo
- Informática – ANIMSA
- Servicios Jurídicos
- Gerencia
- Departamentos de gestión.
- Comisión Técnica de Gestión Documental.

Las funciones y responsabilidades que tendrán cada uno de los agentes implicados en la preservación de los documentos y expedientes electrónicos será:

9.7.1 Archivo

El Archivo tendrá las siguientes funciones:

- Gestionar los documentos y expedientes electrónicos, así como cualquier objeto digital siempre y cuando se haya procedido a hacer la transferencia de éstos al Archivo.
- Dar acceso a los documentos y expedientes electrónicos, así como cualquier objeto digital que se haya transferido al Archivo.
- Operar la plataforma de Archivo.
- Gestionar los usuarios de la plataforma.
- Aceptar las transferencias de los elementos a archivar siempre y cuando éstos cumplan con los estándares definidos en el modelo de gestión documental: formatos, metadatos, tipos de firma electrónica, etc.
- Rechazar las transferencias de los elementos a archivar cuando éstos no cumplan con los estándares definidos en el modelo de gestión documental: formatos, metadatos, tipos de firma electrónica, etc.
- Aplicar los procesos de migración de los objetos digitales guardados en el archivo electrónico cuando éstos tengan problemas de obsolescencia de acuerdo con la Comisión Técnica de Gestión Documental.
- Aplicar los procesos de resellado de firmas electrónicas cuando éstas puedan perder su validación.

- Ejecutar los procesos de verificación de la integridad de los objetos almacenados en el archivo electrónico.
- Gestionar los metadatos asociados a los documentos, expedientes y firmas electrónicas, que se requiera mantener durante la fase de archivo de los objetos.
- Mantener actualizada la información del Cuadro de Clasificación, Calendario de Conservación y del Vocabulario de Metadatos dentro de la plataforma de archivo electrónico.
- Realizar las comprobaciones necesarias en los procesos de migración para garantizar que se ha realizado correctamente el proceso de migración.
- Participar en la Comisión Técnica de Gestión Documental.

9.7.2 Informática - ANIMSA

Informática y en estos momentos ANIMSA tendrá las siguientes funciones:

- Garantizar el servicio de las herramientas tecnológicas necesarias para la gestión de la preservación de los documentos y expedientes electrónicos.
- Actualizar tanto el hardware donde se almacenan los objetos digitales a preservar cuando dicho hardware pueda quedar en desuso o existan nuevos sistemas más rápidos o fiables que los actuales siempre y cuando el presupuesto del Ayuntamiento así lo permita. Ampliarlo cuando se requiera más capacidad de almacenamiento.
- Actualizar el software que va a gestionar todo el archivo electrónico a las nuevas versiones, cuando éstas aparezcan, no más allá de 6 meses desde su aparición.
- Negociar con el fabricante del software o en el caso que sea propio, el desarrollo, de las nuevas funciones de migración de formatos. Este punto es de especial importancia, puesto que los procesos de migración irán evolucionando a medida que aparezcan nuevos formatos.
- Realizar copias de seguridad (semanales, a excepción de cuando se hayan realizado procesos de migración, que será antes y después de este proceso) de los datos, documentos, objetos de la plataforma de archivo electrónico.
- Dar soporte y formación (o en su caso contratar al suministrador de las herramientas esta formación) al Archivo de las funcionalidades de las herramientas y de las nuevas versiones.
- Actuar como administrador de sistemas de la plataforma de archivo electrónico.
- Implementar y garantizar las medidas de seguridad de la plataforma.
- Participar en la Comisión Técnica de Gestión Documental.

9.7.3 Servicios Jurídicos

Los Servicios Jurídicos tendrán las siguientes funciones:

- Dar cobertura jurídica a la plataforma de archivo electrónico a partir de la política de gestión documental.
- Participar en la Comisión Técnica de Gestión Documental.

9.7.4 Gerencia

La Gerencia en el ámbito de la preservación del documento y expediente electrónico tendrá las siguientes funciones.

- Definir los flujos de los procesos que generan los expedientes y documentos electrónicos. Simplificar los procesos actuales.
- Impulsar el procedimiento administrativo y la interoperabilidad con documento electrónico en todos los procesos de digitalización de trámites.
- Participar en la Comisión Técnica de Gestión Documental.

9.7.5 Departamentos de Gestión

Los Departamentos de Gestión del Ayuntamiento tendrán las siguientes funciones:

- Gestionar los documentos y expedientes electrónicos, así como cualquier objeto digital antes de haberse hecho la transferencia de éstos al Archivo.
- Informar al Archivo de los volúmenes de expedientes que se prevé transferir anualmente para que el Archivo pueda dimensionar la plataforma de preservación.
- Informar correctamente de todos los metadatos tanto de documentos, como de expedientes, como de firmas electrónicas en base al vocabulario de preservación.
- Garantizar que las firmas electrónicas son válidas y con el formato correcto antes de ser transferidas.
- Solicitar el proceso de transferencia de los elementos a archivar siempre y cuando éstos cumplan con los estándares definidos en el modelo de gestión documental: formatos, metadatos y tipos de firma electrónica.
- Solucionar los problemas en los objetos que hayan sido rechazados por parte de Archivo en el proceso de transferencia, por no cumplir los estándares fijados. Posteriormente, volver a solicitar la transferencia.

9.7.6 Comisión Técnica de Gestión Documental

La Comisión Técnica de Gestión Documental, cuyas funciones están definidas en el Modelo Organizativo, tiene en el ámbito de la preservación del documento y expediente electrónico, las siguientes funciones:

- Decidir cuándo un formato es obsoleto.
- Definir a que formato se va a migrar un formato que se haya definido como obsoleto.
- Verificar que no hay objetos con formato obsoleto 3 meses después de ser declarado un formato obsoleto y de que se haya implementado en la herramienta de archivo los procesos de migración correspondientes.

10. Modelo de seguridad del documento y expediente electrónico

El Ayuntamiento de Pamplona se dotará de una Política de Seguridad de la Información y determinará los correspondientes procedimientos para su cumplimiento:

- Organización de la Seguridad de la información.
- Seguridad lógica
- Seguridad física
- Explotación, mantenimiento y control de cambios de:
 - Software
 - Hardware
 - Bases de datos
- Desarrollo y mantenimiento de aplicaciones
- Gestión de telecomunicaciones y seguridad perimetral
- Operación de los sistemas informáticos (copias de respaldo y recuperación, gestión de incidencias y control de procesos informáticos)
- Gestión de servicios externalizados
- Continuidad de operaciones
- Cumplimiento normativo

En consonancia con esta Política de Seguridad de la Información, en este capítulo del Plan Director del Documento Electrónico se desarrolla el modelo de seguridad del documento y expediente electrónico (en adelante, modelo de seguridad documental) que tiene por objetivo definir los aspectos específicamente relacionados con la seguridad en el acceso y tratamiento de expedientes y documentos electrónicos. Para el resto de aspectos relacionados con la seguridad de la información será necesario referirse a la Política de Seguridad mencionada.

En este sentido, si partimos de las dimensiones de seguridad establecidas por el Esquema Nacional de Seguridad, que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones, la seguridad de la información aplicada a la gestión documental implica:

- **Autenticidad del documento electrónico:** Se garantiza la fuente de la que proviene la información contenida en un documento, es decir, su autoría, quedando el autor vinculado por las declaraciones contenidas en el documento o los metadatos relacionados. En este sentido, y en sintonía con la norma ISO 15489 de gestión documental, mediante la autenticidad de un documento electrónico se debe poder demostrar que:
 - Es aquello que manifiesta ser;

- Ha sido creado o enviado por la persona que manifiesta haberlo hecho;
- Se ha creado o enviado en el momento en que se manifieste haberlo hecho;
- **Integridad del documento electrónico:** Se mantiene de forma continuada y exacta la información contenida en un documento, es decir, que no ha recibido modificaciones no autorizadas y consiste en un documento electrónico completo e inalterado.
- **Confidencialidad del documento electrónico:** La información de documentos y expedientes electrónicos no se pone a disposición de individuos, entidades o procesos no autorizados o que no necesiten conocerla.
- **Disponibilidad del documento electrónico:** Se provee el acceso y utilización de la información y documentos, e incluso los sistemas informáticos para su tratamiento, por parte de los individuos, entidades o procesos autorizados cuando lo requieran, momento en que se requerirá también de su usabilidad, de manera que pueda ser localizado, recuperado, presentado e interpretado.
- **Trazabilidad del documento electrónico:** las acciones de una entidad sobre un documento pueden ser imputadas exclusivamente a esta entidad y se pueden identificar y reconstruir adecuadamente las acciones que se han hecho sobre el documento, desde su creación y todas sus modificaciones.

Para dar cobertura a estas dimensiones de seguridad, el modelo de seguridad documental del Ayuntamiento de Pamplona va orientado esencialmente a:

- proteger la información confidencial, en general;
- proteger los datos personales de los documentos, en concreto;
- proteger la propiedad intelectual;
- promover la interoperabilidad de confianza;
- apoyar la divulgación y difusión de forma controlada de la información de la cual es responsable.

Adicionalmente, el modelo de seguridad documental del Ayuntamiento de Pamplona se rige por:

- Los principios y normas aplicables a la protección de la confidencialidad y privacidad de datos destacando la Ley Orgánica de Protección de Datos y el Esquema Nacional de Seguridad.
- Los dictámenes del Departamento de Archivo del Ayuntamiento el cual es el encargado de la evaluación y la definición de los criterios de acceso a los documentos.
- Aquello establecido por el presente apartado del Plan Director del Documento Electrónico.

Para dar respuesta a estos requisitos sobre las herramientas de gestión documental del Ayuntamiento, se establecen cuatro procesos clave cuyo objetivo es asegurar un adecuado control de acceso a la información a lo largo de todo el Ciclo de vida de los Documentos y Expedientes electrónicos. Estos cuatro procesos clave se enumeran a continuación junto con la pregunta a la que pretenden dar respuesta:

- **Autenticación de los usuarios:** ¿Quién puede acceder a la plataforma tecnológica de gestión de documentos y expedientes electrónicos?
- **Recuperación de la información y la documentación:** ¿Cómo se asegura la integridad de la información almacenada ante eventuales incidentes de seguridad?
- **Monitorización de la información y la documentación:** ¿Qué se hace sobre la información y cuándo se hace?
- **Acceso a la plataforma tecnológica de gestión de documentos y expedientes electrónicos:** ¿Quién puede hacer qué sobre la información almacenada en la plataforma tecnológica de gestión de documentos y expedientes electrónicos?

En el presente modelo de seguridad del Plan Director del Documento Electrónico del Ayuntamiento de Pamplona se definen estos 4 procesos y finalmente se establecen las directrices sobre las cuales se podrá realizar su aplicación práctica en la plataforma tecnológica de gestión de documentos y expedientes electrónicos del Ayuntamiento de Pamplona.

10.1 Conceptos del modelo de seguridad

Con carácter previo a la definición detallada del modelo de seguridad del Plan Director del Documento Electrónico del Ayuntamiento de Pamplona se procede a continuación a definir una serie de conceptos clave en el ámbito de la seguridad de la información:

- **Aplicación de seguridad:** Directorio de usuarios, donde están registrados todos los usuarios de los sistemas informáticos del Ayuntamiento de Pamplona y el rol de acceso al mismo. Este sistema permite la validación de la identidad del usuario y su rol de acceso para cada acceso que realiza a las distintas aplicaciones que conforman la plataforma tecnológica de gestión de documentos y expedientes electrónicos. Adicionalmente, en este directorio se encuentran informados datos acerca de los usuarios como son el nombre de la persona, el cargo, el departamento al que pertenecen, etc.
- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice que es o bien se garantiza la fuente de la que proviene la información.
- **Confidencialidad:** Propiedad o característica consistente en que la información no es puesta a disposición, ni revelada a individuos, entidades o procesos no autorizados o que no necesitan conocerla.

- **Disponibilidad:** Propiedad o característica consistente en que las entidades o procesos autorizados tienen acceso a la información cuando lo requieren.
- **Integridad:** Propiedad o característica consistente en que la información no ha sido modificada de forma no autorizada.
- **Plataforma tecnológica de gestión de documentos y expedientes electrónicos:** considera
 - la aplicación de gestión de documentos electrónicos ALMADOC
 - cualquiera de las aplicaciones, como es el caso del Gestor de expedientes GEXP, que permiten la creación, introducción y modificación de documentos en los expedientes electrónicos apoyándose en ALMADOC en cuanto a la gestión documental de los mismos.
 - la herramienta de preservación documental a largo plazo en la que se almacenan y conservan aquellos documentos y expedientes con valor histórico.
 - herramientas accesorias a la gestión documental como las de firma electrónica, sellado de tiempo, evidencias electrónicas, etc.
 - las herramientas accesorias que permiten la ejecución de lo anterior, como son sistemas operativos o bases de datos.

Para mayor detalle consultar el capítulo 6 de este Plan Director del Documento Electrónico sobre el modelo tecnológico del documento y expediente electrónico y el capítulo 9 sobre el modelo de preservación de documentos electrónicos a largo plazo.

- **Rol de acceso:** mecanismo de seguridad que permite definir el nivel de acceso de cada usuario a la Plataforma tecnológica de gestión de documentos y expedientes electrónicos. El "rol" debe entenderse como un perfil de usuario, no como un cargo o un puesto de trabajo.

Las personas con el mismo "rol" compartirán responsabilidades y permisos funcionales sobre la plataforma tecnológica de gestión de documentos y expedientes electrónicos y tendrán asociado un conjunto de acciones a poder llevar a cabo sobre las series documentales y sobre los expedientes electrónicos relacionados y sus respectivos documentos electrónicos.

- **Sistema:** Conjunto de herramientas tecnológicas, metodológicas, políticas, etc. que se han creado para un fin concreto.
- **Sistema de seguridad:** Conjunto de herramientas, tecnológicas, metodológicas, políticas de seguridad, etc. que permiten garantizar un nivel de seguridad determinado en una organización.
- **Sistema de gestión documental:** Conjunto de herramientas, tanto tecnológicas como metodológicas así como políticas y modelos específicos para la gestión de

los documentos y expedientes electrónicos así como su clasificación, metadatos, formatos, tipologías, firmas electrónicas, ...

- **Sistema de autenticación:** Herramienta que permite identificar a los usuarios y a su vez determinar los permisos que tienen para acceder a los documentos o realizar procesos con ellos.
- **Trazabilidad:** Propiedad o característica consistente en que las acciones de una entidad pueden ser imputadas exclusivamente a esta entidad y se pueden identificar y reconstruir adecuadamente las acciones que se han hecho sobre la información

10.2 Autenticación de los usuarios

Para identificar inequívocamente a las personas que acceden a la plataforma tecnológica de gestión de documentos y expedientes electrónicos, es necesario disponer de una funcionalidad de autenticación de usuarios. En el caso del Ayuntamiento de Pamplona, esta Plataforma tecnológica está integrada con la plataforma de gestión de usuarios y perfiles del Ayuntamiento denominada “Aplicación de Seguridad” la cual, a su vez, está integrada con el Directorio Activo de MS Windows que permite la gestión del control de acceso de los usuarios a los distintos entornos informáticos de gestión mediante el uso de contraseñas seguras que son renovadas periódicamente por los usuarios, según establece la Política de Seguridad de la Información. Los objetivos fundamentales de estas integraciones son:

- Permitir la validación de todo usuario que intente acceder a la Plataforma tecnológica de gestión de documentos y expedientes electrónicos y permitirle acceso a recuperar información y documentación en consonancia con los permisos de que disponga.
- Permitir realizar las acciones sobre la información y documentación que el usuario tenga capacidad según los permisos asignados.
- No permitir al usuario acceder a o realizar actuaciones sobre información y documentación a la que tenga acceso si no tiene los permisos de edición suficientes e informar debidamente de ello al usuario.
- Informar al usuario en caso de que intente acceder a una información dañada ya sea porque se ha corrompido, se haya perdido información, haya modificado indebidamente o no se pueda validar.

Para asegurar estas premisas, la autenticación de los usuarios a la plataforma tecnológica de gestión de documentos y expedientes electrónicos se llevará a cabo, siempre, de forma nominal con el propio usuario de cada persona con acceso autorizado a la Plataforma tecnológica de gestión de documentos y expedientes electrónicos. Por lo tanto, los usuarios genéricos quedan terminantemente prohibidos a no ser que cada acción realizada por los

mismos pueda ser asociada inequívocamente a una persona o proceso del sistema informático que las haya ejecutado.

Adicionalmente, la autenticación de los usuarios se realizará mediante tres vías principales, siendo:

- **Autenticación de los usuarios sobre las aplicaciones de tramitación de expedientes electrónicos.** Los usuarios responsables de la tramitación de expedientes se autenticarán, a través de la “Aplicación de Seguridad”, sobre las herramientas que permiten llevar a cabo las tareas de tramitación correspondientes. Estas herramientas accederán, por el medio que se determine pudiendo ser por ejemplo servicios web, a la documentación almacenada en la plataforma tecnológica de gestión de documentos y expedientes electrónicos en base a los permisos otorgados al usuario en la aplicación de gestión de expedientes correspondiente.
- **Autenticación de los usuarios sobre las herramientas tecnológicas de gestión de documentos y expedientes electrónicos.** El personal responsable del Departamento de Archivo del Ayuntamiento, es decir, con plena competencia en las fases de vigencia y de valor histórico o permanente de la documentación electrónica, se autenticarán, a través de la “Aplicación de Seguridad”, a la aplicación de gestión de documentos electrónicos, ALMADOC, y la herramienta de preservación de documentos electrónicos. Estas herramientas permitirán establecer perfiles de acceso en función de series documentales siendo siempre accesos de lectura ya que la modificación se realizará mediante las herramientas de gestión de expedientes electrónicos durante la fase de tramitación o, en caso de expedientes cerrados que deben permanecer inalterables, si el personal de Archivo autoriza su reapertura (ver capítulo 6 sobre el modelo tecnológico).
- **Acceso vía plataforma de interoperabilidad.** En el caso de que otras Administraciones Públicas puedan requerir documentación emitida por el Ayuntamiento, con el objetivo de reducir cargas administrativas, se prevé la posibilidad de acceso a través de vías de interoperabilidad. En este caso, el control de acceso se basará en identificación basada en certificado digital de aplicación y garantizará que sólo tengan acceso aquellas Administraciones Públicas con las que se haya suscrito el correspondiente convenio y el interés legítimo de la otra Administración Pública en acceder a la información, guardándose la debida constancia de ello, así como de la información accedida y del momento del acceso.

10.3 Recuperación de la información y la documentación

En el tratamiento de información y documentación en soporte electrónico resulta clave disponer de un servicio de respaldo que permita su recuperación en el estado más próximo al momento en el que sucedió un incidente de seguridad con efecto sobre la integridad de la información.

Según esta premisa, todo elemento que participe en la gestión de documentos y expedientes electrónicos debe:

- Permitir guardar todos los expedientes y sus documentos y firmas electrónicas y metadatos asociados.
- Disponer de procesos automáticos de copias de seguridad y de recuperación.
- Permitir definir la ubicación sobre la que se realizará y recuperará la copia.
- Permitir a un rol administrador la posibilidad de acceder a y restaurar las copias de seguridad.
- Avisar a los usuarios automáticamente en caso de realizarse un proceso de restauración y facilitar información relativa a la situación en qué ha sido recuperada la documentación y la información que la integra.

En este sentido es necesario asegurar la correcta aplicación de los procedimientos de copias de respaldo y recuperación de los sistemas informáticos definida por el Ayuntamiento de Pamplona y que, en la gestión de documentos y expedientes electrónicos, debe sostenerse sobre las siguientes directrices:

- Todos los documentos, metadatos y otros contenidos de carácter documental se almacenan sistemáticamente en los repositorios destinados al efecto, sobre los cuales se aplican los procesos de copia de seguridad y recuperación. No existen documentos o datos relevantes para la gestión documental almacenados de manera temporal o provisional en repositorios que no cumplan con la política de recuperación.
- Existe una clasificación de las copias de seguridad, a fin de posibilitar la identificación de cada una de ellas y su contenido, así como de posibilitar su debida administración.
- Se establecen periodos de sustitución de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados según las recomendaciones del fabricante.
- Se almacenan los documentos de recuperación en una ubicación que cumpla unos requisitos que permitan asegurar su protección y seguridad.
- Se asigna a la información de recuperación las debidas medidas de control de acceso físico y ambiental ubicándose suficientemente alejadas de las instalaciones principales para que un mismo incidente de seguridad no pueda afectar a la información en el entorno de producción y de recuperación.
- Se verifican y se prueban periódicamente los procedimientos de restauración de información garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos según su criticidad.

10.4 Monitorización de la información y la documentación

En la plataforma tecnológica de gestión de documentos y expedientes electrónicos es indispensable disponer de mecanismos que permitan validar qué acciones se realizan sobre él y asegurar su correcto funcionamiento, con el objetivo de validar que tanto la propia plataforma tecnológica como los usuarios que actúan pueden realizar sus actividades de forma correcta y en el tiempo adecuado.

En este sentido es necesario que dicha Plataforma tecnológica sea monitorizada en dos aspectos primordiales:

- **Uso:** registro de las actividades sucedidas sobre la Plataforma tecnológica por parte de los usuarios y procesos automáticos que garanticen la trazabilidad de las actuaciones sucedidas en la Plataforma y obtener estadísticas sobre su uso.
- **Operación:** actividades encaminadas a asegurar el correcto mantenimiento y explotación de la Plataforma tecnológica para garantizar el correcto desempeño de las funcionalidades que le son atribuidas.

Seguidamente se definen estos aspectos con mayor profundidad.

10.4.1 Uso de la Plataforma tecnológica de gestión de documentos y expedientes electrónicos

El control y seguimiento del uso de la plataforma tecnológica de gestión de documentos y expedientes electrónicos se llevará a cabo a través de un conjunto de indicadores de la Plataforma tecnológica. Estos indicadores se dividirán en dos ámbitos diferentes:

- **Indicadores unitarios:** Permiten realizar el seguimiento de qué acciones se realiza sobre los documentos y expedientes de la Plataforma tecnológica. Con estos indicadores será posible determinar quién, cuándo y qué se ha hecho sobre la Plataforma tecnológica en un momento concreto y para un expediente o documento concreto.

Para no afectar al rendimiento de la Plataforma tecnológica, ya que a mayor nivel de auditoría menor rendimiento de la misma, se plantea un nivel de auditoría medio-alto, donde los indicadores unitarios que se registren sean:

- Accesos a la Plataforma tecnológica
- Creaciones de objetos, entendiéndose objeto como expediente, documento o firma electrónica.
- Eliminación de objetos
- Versionado de documentos.
- Cambios en el valor de aquellos metadatos que participen en el control de acceso a documentos y expedientes electrónicos, concretamente el nivel de acceso con posibles valores: público, restringido o confidencial.

- Modificaciones sobre los roles de acceso de los usuarios.
- Modificaciones de usuarios con acceso confidencial a un expediente electrónico.
- Actuaciones realizadas por los usuarios con capacidad de administración de la plataforma tecnológica de gestión de documentos y expedientes electrónicos.
- **Indicadores volumétricos:** Permiten dar una visión en conjunto sobre cuál es el uso de la Plataforma tecnológica. Con estos indicadores se debe disponer de información estadística útil para el análisis de la Plataforma tecnológica en los ámbitos de:
 - Trazabilidad. Actuaciones realizadas sobre objetos, usuario responsable de la actuación y momento en el que suceden.
 - Uso. Acceso y modificación de expedientes y documentos electrónicos realizada por un usuario.
 - Tiempo. Durante el cual se accede o modifica un expediente o documento electrónico por parte de un usuario.

10.4.2 Operación de la Plataforma tecnológica de gestión de documentos y expedientes electrónicos

Como cualquier otro sistema informático, la plataforma tecnológica de gestión de documentos y expedientes electrónicos requiere de una supervisión mediante procesos de monitoreo continua que registren información sobre su funcionamiento útil para asegurar su correcta ejecución.

Estos procesos de monitoreo son procedimientos internos de la Plataforma tecnológica, transparentes para el usuario final, que estarán bajo el control del rol de Administrador tecnológico de la Plataforma y se llevarán a cabo de forma periódica.

Estos procedimientos, que se definen específicamente para cada sistema informático involucrado en el tratamiento de expedientes y documentos electrónicos en el procedimiento de explotación correspondiente, contemplarán como mínimo las siguientes acciones:

- Ejecución de procedimientos de monitorización y revisión para:
 - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
 - Identificar incidencias e información útil para su resolución.
 - Determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación al previsto.

- Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
- Revisar regularmente la efectividad del sistema informático.
- Revisión, en intervalos planificados, de las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles y el entorno exterior tal y como establece la Política de Seguridad del Ayuntamiento.
- Realización periódica de auditorías internas y externas de seguridad y actualización de los planes de seguridad en función de las conclusiones y nuevos hallazgos.
- Registro y revisión proactiva de acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del sistema informático.

10.5 Acceso a la plataforma tecnológica de gestión de documentos y expedientes electrónicos

La plataforma tecnológica de gestión de documentos y expedientes electrónicos debe asegurar que se pueda restringir y controlar el acceso a los expedientes, a sus documentos y a la información que éstos contienen.

Según esta premisa, la Plataforma tecnológica de gestión de documentos y expedientes electrónicos debe:

- Permitir disponer de un perfil de Administrador tecnológico de la Plataforma que pueda configurar los niveles de seguridad de cada elemento participante en la gestión de documentos y expedientes electrónicos.
- Identificar los usuarios impidiendo el acceso en caso de no estar autorizados ya sea porque su nivel de acceso no lo permita o, aun teniendo el nivel de acceso adecuado, no dispongan de acceso confidencial a un expediente clasificado con este nivel de seguridad.
- Restringir el acceso a ciertos documentos o expedientes, componentes del cuadro de clasificación documental según el nivel de acceso del usuario y, a ciertos documentos o expedientes, según su nivel de seguridad.
- Establecer un grupo de usuarios asociado a Series documentales. Si un usuario no tiene asociado el acceso a una Serie documental tampoco podrá acceder a los expedientes relacionados y la documentación que contengan.
- Asignar niveles de seguridad a los expedientes y documentos en función de su clasificación de seguridad según el Cuadro de Clasificación del Ayuntamiento.
- Permitir asignar un usuario a un grupo de usuarios con el mismo nivel de acceso.
- Permitir que un usuario pertenezca a más de un grupo.

- Vetar el acceso a los expedientes o los documentos electrónicos conforme los niveles de seguridad asignados.
- Si un usuario busca textos contenidos en metadatos o documentos correspondientes a expedientes a los que no tiene acceso no se debe permitir su visualización. Para el usuario este expediente no existe y, por lo tanto, la búsqueda no debe devolver resultados relacionados con el expediente ni con el contenido del mismo.
- Permitir que la clasificación de seguridad asignada varíe temporalmente de forma automática en función de determinados parámetros o metadatos del expediente o sus documentos.
- Permitir asignar a expedientes concretos niveles de seguridad más restrictivos que la serie documental a la que pertenecen.
- Evitar que se pueda asignar un nivel de seguridad inferior a un expediente y uno superior a sus documentos o viceversa. La clasificación del nivel de seguridad siempre quedará establecida a nivel de expediente para todo su contenido.

Para cumplir con estos requisitos, hay que dar respuesta a dos preguntas primordiales:

- ¿Qué se puede hacer a nivel funcional?
- ¿Cuándo se puede hacer?

La respuesta a estas dos preguntas, se estructura en dos modelos que se combinan entre sí, para constituir el modelo de restricción de acceso que se aplicará en todos los elementos participantes en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos durante todo su ciclo de vida. Estos modelos son, respectivamente a cada pregunta: Roles de acceso y Niveles de seguridad, según se describe a continuación.

10.5.1 Roles de acceso

Para permitir la flexibilidad en la gestión del acceso a la Plataforma tecnológica de gestión de documentos y expedientes electrónicos y garantizar que cada usuario dispone del nivel de acceso que le confiera acceso sólo a aquella información que requiere para el desempeño de sus funciones, la gestión del acceso se llevará a cabo mediante un modelo de seguridad documental basado en roles.

El "rol" debe entenderse como un perfil de usuario, no como un cargo o un puesto de trabajo. Las personas con el mismo "rol" compartirán responsabilidades y permisos funcionales sobre la plataforma tecnológica de gestión de documentos y expedientes electrónicos.

Cada uno de estos roles tienen asociado un conjunto de acciones a poder llevar a cabo sobre las series documentales y, evidentemente, sobre los expedientes electrónicos y sus respectivos documentos electrónicos.

Existen 2 tipos de roles según su ámbito de aplicación, ya sea a nivel de serie documental o a nivel de todas las series documentales de la plataforma tecnológica de gestión de documentos y expedientes electrónicos.

De acuerdo con esta clasificación, los roles de la plataforma tecnológica de gestión de documentos y expedientes electrónicos son los que se muestran en la siguiente tabla, identificándose sus permisos funcionales en las fases del ciclo de vida del documento y expediente electrónico, y se describen en los siguientes subapartados.

Estos roles de acceso vinculados a las series documentales que establece el Cuadro de Clasificación del Ayuntamiento de Pamplona permiten dar respuesta a la gestión completa del ciclo de vida del documento y expediente electrónico garantizando que cada usuario de la Plataforma tecnológica de gestión de documentos y expedientes electrónicos dispondrá del nivel de acceso necesario para el desempeño de sus funciones.

Grupo de usuarios	Fase de tramitación			Fase de vigencia y archivo	
	Consulta	Modificación	Eliminación	Consulta	Eliminación
Ámbito de aplicación del rol: a nivel de serie documental					
Equipo de tramitación	Sí	Sí	Sí	Sí	No
Consulta restringida	Sí	No	No	Sí	No
Superior inmediato	Sí	No	No	Sí	No
Consulta pública	Sí	No	No	Sí	No
Aplicación	Sí	Sí	Sí	Sí	No
Ámbito de aplicación del rol: a nivel de todas las series documentales					
Administrador del archivo	A partir de la solicitud de transferencia a Archivo del expediente	No	No	Sí	Sí
Administrador tecnológico	Sí	Sí	Sí	Sí	Sí

10.5.1.1 Roles de serie documental

Los roles de serie documental tienen las siguientes propiedades:

- Los usuarios tienen acceso a series documentales mediante la atribución de roles de acceso.
- Se asignan a todas las series documentales relacionando series documentales con roles de acceso.
- Cada serie documental se puede configurar por separado.
- Cada rol dispone de un conjunto de permisos propio sobre un conjunto de series y fase del ciclo de vida del documento y expediente electrónico, pudiendo ser de consulta, modificación y eliminación.
- Los permisos de cada rol son los mismos para cada serie que dispongan relacionada.
- A los roles se asignan aquellos usuarios o grupos de usuarios pertinentes para cada serie.

De acuerdo con ello, se definen los siguientes grupos de usuarios:

- **Equipo de tramitación:** Es el equipo responsable de la tramitación de los expedientes de un procedimiento del Ayuntamiento. Tiene la potestad de crear expedientes y, mientras permanezcan abiertos, de:
 - Editar los metadatos editables del expediente, entre ellos el siguiente relevante a efectos de seguridad:
 - El metadato de nivel de acceso sobre el carácter de público, restringido y confidencial de un expediente (ver apartado 10.5.2 sobre niveles de seguridad).
 - Crear, introducir y modificar documentos en el expediente.
 - Editar los metadatos editables de los documentos, entre ellos los siguientes relevantes a efectos de seguridad:
 - La determinación del estado definitivo de un documento por el cual el documento será incorporado al sistema informático de gestión documental ALMADOC y no podrá ser eliminado.
 - El carácter confidencial de un documento que convertirá al conjunto del expediente en confidencial (ver apartado 10.5.2 sobre niveles de seguridad) y por el cual sólo los usuarios que hayan participado en la tramitación del expediente y quienes éstos determinen dispondrán de acceso al mismo, aunque pertenezca a un expediente de una serie a la que disponen de acceso de tramitación o de consulta, restringida o pública, más usuarios.
 - Eliminar documentos del expediente no considerados como definitivos.

- Cerrar el expediente.
- **Consulta restringida:** Dispondrá de permisos para consultar el expediente y sus respectivos documentos y metadatos, pero no editarlos ni añadir documentos adicionales. En la mayoría de casos estará formado por las mismas personas que conforman el equipo de tramitación que dispondrán de acceso a expedientes cerrados, en fase de vigencia y archivo, o por personas que para el desempeño de sus funciones requieren de acceso de consulta a los expedientes de una serie documental, tanto en fase de tramitación como de vigencia y archivo. Tiene la potestad de:
 - Consultar documentos.
 - Consultar metadatos de expediente.
 - Consultar metadatos de documento.
- **Superior inmediato:** Es el rol que permite consultar los expedientes y los documentos de las series de las cuales se es responsable funcional, exceptuando aquellos clasificados como confidenciales, pero no permite su modificación ni tampoco su eliminación. Tiene las mismas potestades que el rol de consulta restringida y para tener acceso a aquellos expedientes y documentos calificados como confidenciales deberá disponer del acceso confidencial al mismo.
- **Consulta pública:** Rol similar al de consulta restringida, pero reservado a la consulta de documentos y expedientes de toda la Plataforma tecnológica de gestión de documentos y expedientes electrónicos siempre que sean calificados como de acceso público a través del metadato correspondiente. Tiene la potestad de:
 - Consultar documentos.
 - Consultar metadatos de expediente.
 - Consultar metadatos de documento.
- **Aplicación:** Rol especial con permisos similares al Equipo de tramitación que permite la interacción automática de herramientas informáticas verticales de gestión de expedientes, como es el caso de GEXP, con el sistema informático de gestión documental ALMADOC para aquellas series documentales con las que opere y partiendo de la base de la gestión de permisos de usuario establecida en la aplicación de gestión de expedientes. Tiene la potestad de:
 - Crear expedientes.
 - Editar los metadatos del expediente.
 - Crear, introducir y modificar documentos en los expedientes.
 - Editar los metadatos de los documentos, entre ellos, la determinación del estado definitivo de un documento.
 - Eliminar documentos del expediente no considerados como definitivos.

- Cerrar el expediente.

10.5.2 Roles de la plataforma tecnológica de gestión de documentos y expedientes electrónicos

Los roles de la plataforma tecnológica de gestión de documentos y expedientes electrónicos son el conjunto de roles que tienen aplicación sobre toda la plataforma tecnológica de gestión de documentos y expedientes electrónicos, es decir, no están asociados a una serie documental concreta, sino a todas. Estos roles son:

- **Administrador del archivo:** Es el responsable de la conservación y custodia de los expedientes y sus documentos y de organizar la plataforma tecnológica de gestión de documentos y expedientes electrónicos. Dispone de todos los permisos y todos los roles sobre todas las series documentales, una vez se produce el cierre del expediente. Por lo tanto, tiene las mismas potestades que el rol de consulta restringida incluyendo la posibilidad de:
 - Reabrir un expediente para la inclusión de documentación adicional, siempre de forma excepcional y contando con la debida justificación que deberá quedar reflejada en la plataforma tecnológica de gestión de documentos y expedientes electrónicos.
 - Eliminar expedientes dando cumplimiento a la tabla de evaluación documental aplicable a la serie documental a la que pertenece.
 - Realizar transferencias de expedientes a la herramienta de preservación documental.
- **Administrador tecnológico:** El administrador tecnológico es una figura que debe estar presente para garantizar el correcto funcionamiento de un sistema informático en caso de que se produzca un error o malfuncionamiento. Desde el punto de vista funcional, puede no ser necesario, pero a nivel técnico resulta indispensable.

Este perfil posee todos los permisos y todos los roles en cualquier momento del ciclo de vida del documento y expediente electrónico (tramitación, vigencia y archivo) y se encarga de otorgar y mantener los roles de acceso a los usuarios siguiendo las instrucciones de los responsables funcionales.

Las actuaciones de los usuarios con este perfil sobre los expedientes y documentos electrónicos deberán ser monitorizadas para asegurar que sean las mínimas necesarias y respondan siempre a peticiones realizadas por los usuarios responsables de las series documentales (superior inmediato) o el administrador del archivo.

10.5.3 Niveles de seguridad

Los niveles de seguridad de la plataforma tecnológica de gestión de documentos y expedientes electrónicos se definen en dos ámbitos: ámbito de Serie documental y de los expedientes que la conforman y ámbito de Documento.

En cuanto al ámbito de Serie documental y de los expedientes que la conforman, se definen tres niveles de seguridad que se propagan a los documentos que lo conforman:

- **Libre acceso:** La información contenida en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos pertenecientes a este nivel es de libre acceso para todos los usuarios de la Plataforma. Excepcionalmente, un expediente de una Serie de libre acceso podrá ser configurado como de acceso restringido o confidencial dejando constancia de los motivos que lo justifican.
- **Restringido:** La información contenida sólo es accesible para un grupo de usuarios reducido, correspondiente al equipo de tramitación o de consulta restringida, además de los usuarios de la serie documental correspondientes a Superior inmediato y Aplicación, el Administrador tecnológico y, al cierre del expediente, el Administrador del archivo. Excepcionalmente, un expediente de una Serie de acceso restringido podrá ser configurado como de acceso confidencial dejando constancia de los motivos que lo justifican.
- **Confidencial:** La información contenida en un expediente concreto sólo es accesible por las personas que hayan participado directamente en su tramitación, y quienes éstos determinen, aunque el expediente pertenezca a una serie a la que disponen de acceso, restringido o público, más usuarios. Estos usuarios podrán pertenecer al grupo de usuarios del Equipo de tramitación o de Consulta restringida.

Asimismo, el responsable tecnológico y, una vez cerrado el expediente, también el responsable de archivo, podrán acceder a un expediente calificado como de confidencial para la ejecución de las funciones que les son atribuidas debiendo quedar estos accesos debidamente registrados en el sistema para garantizar su posterior monitorización.

Finalmente, el usuario Aplicación con acceso a la Serie documental podrá acceder en el caso de realizar procedimientos automatizados y para conferir el acceso al expediente a aquellos usuarios de aplicaciones de gestión de expedientes que mediante la gestión de permisos de la misma dispongan de acceso confidencial al expediente.

De la misma forma, con respecto al ámbito de los documentos, también tendrán tres niveles de seguridad, independientemente del nivel de Serie documental o Expediente asignado, siendo en cualquier caso de igual o mayor restricción que el de Serie documental o Expediente:

- **Documentos públicos.** Los documentos públicos son aquellos que en su estado definitivo son visibles por la ciudadanía en general, así como por todos los usuarios de la Plataforma tecnológica de gestión de documentos y expedientes electrónicos.

Durante su elaboración (estado borrador, según el metadato correspondiente) su tratamiento será de documento reservado o confidencial, según se determine en cada caso.

- **Documentos reservados:** Documentación generada por el Ayuntamiento de Pamplona o aportada por el ciudadano de uso interno en la Serie documental o Expediente. No es visible ni por los interesados ni por los ciudadanos sino sólo por los usuarios internos con acceso a la documentación contenida en la Serie documental en cuestión, pudiendo pertenecer al grupo de usuarios de Equipo de tramitación o de Consulta restringida. Asimismo, podrán acceder además los usuarios de la serie documental correspondientes a Superior inmediato y Aplicación, el Administrador tecnológico y, al cierre del expediente, el Administrador del archivo.
- **Documentos confidenciales:** Documentación generada por el Ayuntamiento de Pamplona o aportada por el ciudadano de uso interno en la Serie documental o Expediente. No es visible ni por los interesados ni por los ciudadanos sino sólo por los usuarios internos que hayan participado en su tramitación o quienes éstos determinen, aunque el documento pertenezca a un expediente de una serie a la que disponen de acceso, restringido o público, más usuarios. Los usuarios con acceso podrán pertenecer al grupo de usuarios del Equipo de tramitación o de Consulta restringida.

Asimismo, el Responsable tecnológico y, una vez cerrado el expediente, también el Administrador del archivo, podrán acceder a un documento calificado como confidencial para la ejecución de las funciones que les son atribuidas debiendo quedar estos accesos debidamente registrados en el sistema para garantizar su posterior monitorización.

Finalmente, el usuario Aplicación con acceso a la Serie documental podrá acceder en el caso de realizar procedimientos automatizados y para conferir el acceso al documento a aquellos usuarios de aplicaciones de gestión de expediente que mediante la gestión de permisos de la misma dispongan de acceso confidencial al documento.

De acuerdo con esta clasificación de niveles de seguridad y el conjunto de roles definidos, se pueden definir los niveles de seguridad de la Plataforma tecnológica de gestión de documentos y expedientes electrónicos y sus respectivas políticas de seguridad para cada serie documental.

10.5.4 Representación gráfica

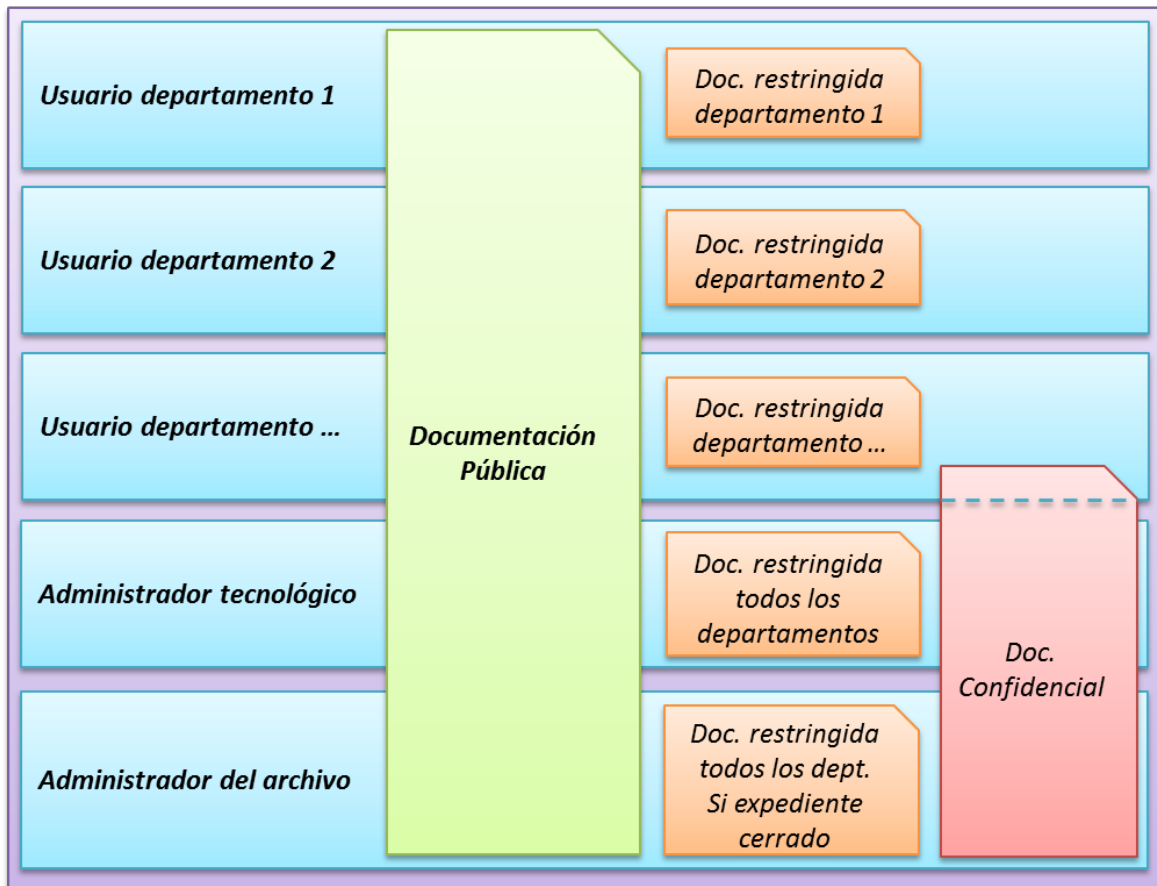
A continuación, se incluye una representación gráfica de la gestión de acceso a la plataforma tecnológica de gestión de documentos y expedientes electrónicos. Siguiendo lo que se acaba de exponer, el presente gráfico tiene por objetivo transmitir gráficamente que

para conferir acceso a un expediente electrónico habrá que responder a dos preguntas básicas:

- Si el usuario dispone de acceso funcional a la documentación, ya sea porqué pertenezca a los grupos de usuarios con acceso restringido a la serie documental a la que pertenece el expediente: equipo de tramitación, grupo de usuarios de consulta restringida, superior inmediato o aplicación. Ello se gestionará a partir de roles de acceso.
- Si el usuario, aun disponiendo del acceso funcional anterior, dispone del nivel de acceso suficiente para un expediente clasificado como confidencial, es decir, que haya participado en su tramitación o, en su defecto, un usuario que haya participado en la tramitación le haya conferido acceso. Ello se gestionará a partir de los metadatos del expediente y del documento electrónico.

En cualquier caso, todo usuario dispondrá de acceso a la documentación calificada como de acceso público y los usuarios:

- Administrador tecnológico, podrá acceder a toda la documentación, incluida la calificada como confidencial, durante todo el ciclo de vida del expediente.
- Administrador del archivo, podrá acceder a toda la documentación, incluida la calificada como confidencial, a partir del cierre del expediente.



10.6 Aplicación del modelo de seguridad documental

Una vez expuesto el modelo de seguridad documental, es conveniente definir las directrices sobre las cuales se podrá realizar su aplicación práctica en la plataforma tecnológica de gestión de documentos y expedientes electrónicos del Ayuntamiento de Pamplona. Estas directrices se incluyen a continuación:

1. La **responsabilidad** de la gestión de la consulta de los documentos corresponderá al departamento responsable según determine el usuario Superior inmediato o responsable funcional asignado a cada Serie documental. Una vez cerrados los expedientes, en su fase de vigencia y archivo, será responsabilidad del Departamento de Archivo quien:
 - a. Resolverá sobre las peticiones de acceso por parte de usuarios de la serie documental distintos a los del Equipo de tramitación, Consulta restringida, Superior inmediato y Aplicación ya que los accesos por parte de estos usuarios no deberán ser autorizados al haber participado durante la fase de tramitación. Tampoco se autorizarán los accesos de los roles de Consulta pública y Administrador tecnológico, aunque los de este último deberán quedar registrados para su posterior monitorización.

- b. De forma excepcional, tendrá la posibilidad de autorizar la reapertura de un expediente para que el personal asignado al equipo de tramitación o, si el expediente es confidencial, aquellos usuarios con acceso confidencial puedan añadir nueva documentación.
2. El acceso a los documentos electrónicos, durante la fase de tramitación, se determinará en base al **cuadro de clasificación de la documentación** del Ayuntamiento a nivel de los expedientes de la Serie documental. Cada Serie documental tendrá asociado:
 - a. Un Departamento que será el responsable funcional y con el que será necesario confirmar cualquier aspecto relacionado con los criterios de gestión y acceso aplicables a la Serie. Esta responsabilidad recaerá sobre el responsable del Departamento en cuestión y se plasmará en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos con el rol de Superior inmediato.
 - b. Los usuarios del departamento funcional y de otros departamentos que participen en la tramitación de los expedientes asociados a la Serie y que se plasmarán en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos con el rol de Equipo de tramitación.
 - c. Los usuarios de otros departamentos que requieran tener acceso de consulta de los expedientes asociados a la Serie y que se plasmarán en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos con el rol de Consulta restringida.
3. El catálogo de procedimientos del Ayuntamiento describirá todos los trámites y fases de cada procedimiento y los perfiles de usuario y el departamento al que pertenecen y que podrán participar accediendo o modificando los documentos de los expedientes asociados al procedimiento.

Asimismo, el catálogo recogerá los documentos y actos de comunicación asociados a los mismos, de forma que se puedan identificar los documentos mínimos que conformaran cada expediente en su fase de tramitación, así como en su fase de vigencia y archivo, una vez cerrado y foliado el expediente.

A su vez, cada expediente y documento electrónico tendrá asignados un conjunto de metadatos descriptivos de su contenido y de otros aspectos del mismo según el **catálogo de metadatos** del Ayuntamiento. Para estos metadatos, el catálogo de procedimientos especificará para cada documento electrónico el valor a asignar a aquellos metadatos cuyo valor sea uniforme para todos los expedientes y documentos de un procedimiento o la forma de obtenerlo durante su tramitación. En lo que respecta a los metadatos de gestión del control de acceso, necesariamente se tendrá en cuenta:

- La determinación general del tipo de acceso otorgado: público, reservado o confidencial. Ello podrá ser modificado por el equipo de tramitación a nivel del expediente electrónico que lo conforman. En el caso de documentos que deban considerarse de tipo de acceso confidencial, todo el conjunto del expediente al que pertenecen pasará a ser clasificado como de nivel confidencial.
- Las razones aplicables para la limitación de acceso por parte del Equipo de tramitación definidas de forma específica para cada expediente o documento electrónico. Ello es de aplicación en el caso excepcional que un expediente de una serie de acceso público se determine por el Equipo de tramitación o Superior inmediato de la Serie como de acceso restringido o una serie de acceso público o restringido se determine como confidencial. En cualquier caso, un expediente o documento no será de acceso público hasta que esté en estado cerrado o definitivo.
- La limitación a las reproducciones del documento.
- En su caso, la presencia en el contenido de datos de carácter personal y el nivel de las medidas de seguridad aplicables a los mismos siendo de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

En los casos en que el valor de los metadatos de un expediente o documento electrónico no quede fijado en el catálogo de procedimientos y tampoco se le hayan atribuido de forma expresa, el valor asignado por defecto deberá ser tal que impida los accesos indebidos a su información. Sin embargo, el personal del Ayuntamiento actuará con la debida diligencia para evitar que la aplicación de este principio deje sin efecto, en su caso, los derechos de consulta y de acceso a la información administrativa por parte de la ciudadanía como parte interesada.

4. El acceso a los documentos nominativos, es decir, aquellos expedidos o asociados a una persona concreta, a los documentos que contengan datos relativos a la intimidad de las personas, y a los expedientes no finalizados queda reservado a las personas que participen en su elaboración, así como las que acrediten las condiciones previstas por la ley en cada caso. Para garantizar que el derecho de consulta a través de medios telemáticos sea ejercido por los ciudadanos y las ciudadanas que se encuentran legalmente habilitados o habilitadas para hacerlo, el Ayuntamiento exigirá su **identificación** por medio de cualquier procedimiento de identificación segura, electrónico o, en su defecto, presencial.
5. En lo que respecta al **acceso a la plataforma tecnológica de gestión de documentos y expedientes electrónicos del Ayuntamiento por parte del personal del Ayuntamiento** se establecen los siguientes criterios de aplicación:

- Para que un usuario pueda acceder a la Plataforma tecnológica de gestión de documentos y expedientes electrónicos del Ayuntamiento deberá superar un proceso de identificación (por ejemplo, a través de un identificador de usuario), autenticación (por ejemplo, a través de una contraseña) y autorización (por ejemplo, a través de roles de acceso y niveles de seguridad que determinen a qué series documentales y expedientes tendrán acceso los usuarios y con qué potestades).
- Los usuarios, salvo situaciones excepcionales que se deberán identificar y aprobar, dispondrán de un identificador de usuario unívoco.
- Las credenciales de acceso de cada usuario son personales e intransferibles, y su proceso de asignación y comunicación garantizará la confidencialidad y prevendrá el acceso no autorizado a través de la suplantación de identidad.
- Los usuarios serán responsables de preservar la confidencialidad de las contraseñas y asegurar el uso correcto de los sistemas informáticos a los que tienen acceso, así como de cualquier otro mecanismo de control de acceso a los mismos como podría ser el certificado digital.
- Los usuarios tendrán acceso a la plataforma tecnológica de gestión de documentos y expedientes electrónicos del Ayuntamiento hasta el momento que lo precisen para el desarrollo de sus funciones. Se preverán procedimientos específicos para controlar la vigencia de los usuarios temporales como, por ejemplo, personal externo. Se mantendrá, por tanto, un listado actualizado de usuarios con acceso autorizado a cada sistema informático participante en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos.
- Cada usuario tendrá acceso a los documentos y expedientes de la Series documentales que precise sobre la base de las necesidades derivadas de sus funciones y responsabilidades, de acuerdo con el análisis que se haya hecho de los procedimientos del Ayuntamiento según figure en su catálogo de procedimientos. Se aplicarán los niveles de acceso: Equipo de tramitación o Consulta restringida.
- La concesión del acceso a los sistemas informáticos de tratamiento de documentos electrónicos del Ayuntamiento lleva asociado un proceso previo formal de solicitud, evaluación y aprobación. Para la aprobación es necesario que se establezcan responsables funcionales de cada Serie documental que decidirán sobre el acceso a los expedientes y documentos pertenecientes a cada Serie documental y sobre los que se aplicará el nivel de acceso: Superior inmediato.
- Siempre que se produzca un cambio en las funciones o responsabilidades de un usuario, se evaluarán sus consecuencias en lo que respecta a

derechos de acceso a los sistemas informáticos de tratamiento de documentos electrónicos del Ayuntamiento.

- Para la definición de los perfiles de acceso a la documentación en formato electrónico, partiendo de lo que establezca el Catálogo de Procedimientos, el Ayuntamiento utilizará las utilidades de segregación de funciones de los sistemas informáticos de tratamiento de documentos electrónicos donde, para cada procedimiento y para cada una de sus fases de tramitación y en consecuencia cada uno de los estados del documento, se determinará qué grupos de usuarios tienen acceso y en qué grado: consulta, modificación y eliminación. Adicionalmente en cada fase del procedimiento se definirá qué documentos serán accesibles, modificables o eliminables quedando prohibida en cualquier caso la eliminación de documentos considerados definitivos. Se establecerán para ello tablas de segregación de funciones que identifiquen todas las transacciones posibles en un sistema informático de tratamiento de documentos electrónicos y cuáles podrán ser ejecutadas por cada tipo de usuario o rol.
- Periódicamente se realizará un proceso de revisión para verificar que sólo los usuarios autorizados tienen acceso a los diferentes sistemas informáticos participantes en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos y que su perfil no exceda las autorizaciones mínimas necesarias para el desarrollo de sus funciones ni se sucedan conflictos de segregación de funciones.
- Se establecerán mecanismos de registro y monitorización de acceso y/o uso de los sistemas informáticos participantes en la Plataforma tecnológica de gestión de documentos y expedientes electrónicos que garanticen que los documentos son protegidos de forma efectiva de usos no autorizados, alteración o destrucción, tal y como ha quedado definido en el apartado 10.4.

11. Política de uso del certificado digital y la firma electrónica

11.1 Introducción.

El Ayuntamiento de Pamplona en su estrategia de implantación de la Administración electrónica en general y en la implantación del documento y expediente electrónico va a requerir el uso de certificados digitales y la implantación de la firma electrónica en los documentos y expedientes, así como el foliado de estos, por lo que requiere de una política de uso del certificado digital y de la firma electrónica que garantice su correcto uso.

En este sentido, en la política se hace un análisis detallado de los diferentes escenarios o casos de uso de firma electrónica que se pueden dar en el día a día del Ayuntamiento para cada uno de los cuales se incluirá, al final del documento, la política que lo regirá.

La implantación de un modelo de firma electrónica necesariamente debe especificar cuáles son los tipos de firma a utilizar a la hora de firmar los documentos electrónicos generados y gestionados por el Ayuntamiento, y por esta razón se incluye tanto una relación de formatos utilizados, como tipos de firma generados o aceptados por el Ayuntamiento.

Otro aspecto importante de los modelos de firma electrónica son los certificados digitales y su uso. Se concretan en esta Política los certificados digitales que el Ayuntamiento admitirá por parte de los ciudadanos y los utilizados los trabajadores del Ayuntamiento y, además, de estos últimos certificados se especificará su ciclo de vida.

Hay que señalar que en este documento se utilizan indistintamente los términos firma digital y firma electrónica, ya que corresponden al mismo concepto.

Para la elaboración de este documento se ha tenido en cuenta lo que el Esquema Nacional de Interoperabilidad establece al respecto y muy concretamente, lo que se define en la Norma Técnica de Interoperabilidad de política de firma electrónica y de certificados digitales de la administración, así como la del expediente electrónico en lo referente a la firma electrónica de los expedientes.

11.2 Objeto

Esta política tiene por objeto establecer el conjunto de criterios comunes asumidos por el Ayuntamiento de Pamplona en relación con la autenticación y el reconocimiento de firmas electrónicas basadas en certificados. En concreto establece las directrices a seguir por el Ayuntamiento de Pamplona respecto al uso de la firma electrónica, en el seno de las aplicaciones corporativas, para garantizar la autenticidad, integridad y conservación de los documentos firmados digitalmente.

Así mismo el objetivo de esta política es establecer qué certificados digitales de ciudadano el Ayuntamiento acepta y qué certificados digitales utilizan los trabajadores del Ayuntamiento y, además, de estos últimos certificados, su ciclo de vida.

Por último, establece las estrategias que el Ayuntamiento para la preservación a largo plazo de las firmas electrónicas.

11.3 Datos identificativos de la política.

Los datos identificativos de la política son:

11.3.1 Identificación de la política

- Nombre del documento: Política de firma electrónica Ayuntamiento de Pamplona.docx.
- Versión: 1
- Fecha de aprobación: x de junio de 2015

Nota: pendiente informar fecha aprobación.

11.3.2 Periodos de validez y transición.

La presente Política de Firma Electrónica del Ayuntamiento de Pamplona entrará en vigor en la fecha de su aprobación y será válida hasta que no sea sustituida o derogada por otra política posterior.

Se podrá facilitar un período de tiempo transitorio para adecuar los diferentes sistemas de firma electrónica y validación de esta utilizados por el Ayuntamiento de Pamplona a las especificaciones de la nueva versión.

Este período de tiempo de transición se deberá indicar en la nueva versión, pasado el cual, solo será válida la versión actualizada.

11.3.3 Identificación del gestor del documento de la política

- Gestor de la política: A determinar.
- Dirección de contacto: A determinar.
- e-mail de contacto: A determinar.

11.4 Conceptos

Se ha creído importante incorporar un capítulo de definición de términos, aplicados en este documento, para hacer más comprensible el documento de Políticas de Firma Electrónica del Ayuntamiento de Pamplona.

Casos de uso de la firma electrónica. En este documento nos referimos a los casos de uso de la firma electrónica, a los escenarios posibles de generación de documentos

electrónicos firmados. Para cada caso de uso se identificarán los formatos de firma electrónica, los posibles niveles de firma, la normativa de firma electrónica a aplicar, etc.

Clases de firma electrónica. En este documento nos referiremos a las clases, a la validez jurídica de la firma electrónica, según se define en la Ley 59/2003 de firma electrónica: firma simple, avanzada y reconocida.

Formato de firma electrónica. Forma en que se codifican las firmas electrónicas. Los formatos más utilizados son los formatos S/MIME, CMS, XAdES, CAdES y PAdES.

Nivel de firma: Con este nombre nos referiremos a si el documento tiene una única firma o múltiples firmas y en este caso si se generan en paralelo o anidadas.

Normativa de firma electrónica. Documentos que detallan las normas relativas a la firma electrónica, organizadas alrededor de los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal,...), definiendo las reglas y obligaciones de todos los actores involucrados en dicho proceso. El objetivo de este proceso es determinar la validez de la firma electrónica para los diferentes tipos de transacción. En el caso del Ayuntamiento de Pamplona se definen cinco tipos de transacción diferente: firma electrónica de un documento electrónico, copia auténtica electrónica de documentos en papel, copia auténtica electrónica de un documento firmado electrónicamente e incorporación de documentos firmados digitalmente por parte del ciudadano.

Tipos de firma: Forma como se relaciona la firma electrónica con el documento firmado: dentro del mismo documento, como un documento a parte o dentro de estructuras XML.

11.5 Normativa aplicable y estándares internacionales.

En este apartado se identifican el conjunto de normativas y estándares internacionales que se han tenido en cuenta para la definición de la presente política de firma electrónica.

La reciente revolución en el uso del documento electrónico es el resultado de la aparición de cambios normativos que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como en la Unión Europea o internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

Algunas de las decisiones que se reflejarán en la política de firma electrónica vienen condicionadas o basadas en esta normativa o estos estándares.

Lo que se presenta a continuación es la identificación de:

- Normas, clasificadas en función de su rango y ámbito territorial, que regulan diferentes aspectos asociados a la firma electrónica.
- Estándares internacionales, clasificados en función de la materia, que han servido para informar a las normas anteriores o que se aplican de manera generalizada en los procesos de gestión del ciclo de vida de la firma electrónica.

Dichas normas y estándares están detallados en el capítulo 2 del Plan Director del Documento Electrónico del Ayuntamiento de Pamplona donde se incluye todo el marco normativo. A continuación, se relacionan pues las distintas leyes, normas y estándares.

11.5.1 Normativa aplicable

- Ley Foral 11/2007 de Implantación de la Administración Electrónica.
- Ley 11/2007 de 22 de junio de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Real Decreto 1720/2007 de Desarrollo Parcial de la Ley 11/2007
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto 3/2010 de 8 de enero del Esquema Nacional de Seguridad.
- Real Decreto 4/2010 de 8 de enero del Esquema Nacional de Interoperabilidad.
- Resolución de 19 de julio de 2011 de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- Resolución de 19 de julio de 2011 de la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- Ley 59/2003 de 19 de diciembre de Firma Electrónica.
- Real Decreto 14/1999 de 17 de septiembre que Regula el uso de la firma electrónica, reconociendo su eficacia jurídica. Prestación al pública de servicios de certificación.
- Ley 15/2015 de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
- Directiva 1999/93/EC de 13 de diciembre del Marco comunitario para la firma electrónica.
- Regulación (EU) 910/2014 de 23 de julio de 2014 sobre identidad electrónica y servicios de confianza para las transacciones electrónicas en el mercado interno relativas a la Directiva 1999/93/EC.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

11.5.2 Estándares internacionales y otras convenciones

- ETSI RFC 2315 (1998), ETSI RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS#7: Cryptographic Message Syntax (CMS)
- ETSI TS 101 733. v.1.6.3, v1.7.4 y v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP
- ETSI TS 101 903 v.1.2.2, v.1.3.2 y 1.4.1: XML Advanced Electronic Signatures (XAdES)
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.
- ISO 19005 (2008): Formato de fichero PDF/A-1
- ISO/TR 18492: 2005- Long-term preservation of electronic document-based Information
- UNE-ISO/TR 13008: 2010- Información y documentación. Conversión de documentos digitales y procesos de migración.
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI);
- Policy requirements for time-stamping authorities.
- ETSI TS 101 861 V1.3.1 Time stamping profile.
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

11.6 Uso de certificados digitales

11.6.1 Certificados admitidos por el Ayuntamiento

El mecanismo de firma digital se sustenta en la existencia de Autoridades de Certificación que emiten certificados digitales y permiten comprobar que un certificado concreto ha estado correctamente emitido y que continúa siendo válido en el momento de su uso, es decir de la firma de un documento. La relación entre la Autoridad de Certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza: los certificados serán aceptados sólo en la medida en que la entidad que lo ha de validar confíe en la honestidad de la Autoridad de Certificación.

En este contexto, el Ayuntamiento debe, según la Ley 15/2015 admitir todos los certificados digitales emitidos por los prestadores de servicios de certificación que hayan realizado la comunicación prevista en el artículo 30.2 de la Ley 59/2003 en el Ministerio de Industria, Energía y Turismo y que cumplan con los estándares de calidad y niveles de seguridad establecidos por dicho Ministerio.

El Ayuntamiento está utilizando la plataforma @firma del Ministerio de Industria, Energía y Turismo para la validación de los certificados, por lo que la aceptación efectiva de certificados vendrá condicionada por la actualización de los servicios de dicha plataforma.

Sin embargo, y debido a la necesidad de instalar las claves públicas de las autoridades de certificación en los diferentes servidores del Ayuntamiento, este proceso se puede dilatar en el tiempo. Inicialmente el Ayuntamiento aceptará los certificados digitales de las siguientes autoridades de certificación:

1. DNI ELECTRÓNICO
2. AC CAMERFIRMA
3. FNMT Clase 2 CA.
4. ACA
5. AC ANCERTCP V2
6. ANF AC
7. BANESTO CA
8. IZEMPE
9. ACCV
10. FIRMAPROFESIONAL
11. SCR

En la Sede Electrónica del Ayuntamiento se publicará la lista de certificados admitidos, que se irá actualizando a medida que se pueda garantizar la seguridad de otros certificados de amplia difusión.

11.6.2 Certificados empleados por el Ayuntamiento

Los empleados del Ayuntamiento que deban firmar documentos digitalmente o tener acceso a determinados servicios o aplicaciones donde se requiera un alto nivel de

autenticación, necesitarán certificados digitales. Para este propósito el Ayuntamiento de Pamplona utilizará certificados de empleado público de AC Camerfirma SA.

El Ayuntamiento es entidad de registro de Camerfirma y, por tanto, puede generar los certificados necesarios para sus empleados.

En lo referente a los sellos electrónicos, el Ayuntamiento utilizará los de Camerfirma y se generarán desde la entidad de registro del Ayuntamiento.

Finalmente, y en cuanto a los sellos de sede electrónica, el Ayuntamiento utilizará principalmente los de Camerfirma.

NOTA: debido a la falta de interoperabilidad de ciertas aplicaciones de las AAPP, el Ayuntamiento también podrá utilizar certificados digitales emitidos por la FNMT y por Seguridad Social, para la relación del Ayuntamiento con otras Administraciones Públicas.

Para el ámbito tributario, podrá utilizar certificados de la FNMT de persona jurídica.

Por lo que respecta al uso de certificados digitales de servidor, los utilizados para el intercambio seguro de información entre AAPP se utilizará también los de Camerfirma, o en su defecto, cualquiera de los emitidos por otras autoridades de certificación que ya tengan un alto nivel de instalación, de sus claves públicas, en los navegadores. Cabe señalar que si bien estos certificados no generan actos jurídicos, se ha considerado oportuno incorporarlos a esta política.

11.7 Ciclo de vida de la firma electrónica: creación, verificación y conservación.

Como ya se ha comentado, el Ayuntamiento tiene un contrato con Camerfirma para la emisión de los certificados digitales que requiera en la realización de sus actividades.

Camerfirma es la responsable de definir las políticas de gestión de los certificados digitales que emite y por tanto es quien define la vigencia de los certificados, la manera como se revocan, se renuevan, se validan, etc.

Para la emisión de certificados digitales del Ayuntamiento este dispone de una Entidad de Registro interna. A efectos de adoptar los procedimientos establecidos por Camerfirma para operar la Entidad de Registro se han establecido procedimientos internos que identifican las actividades que se realizan y sus responsables, así como los procedimientos a seguir por los usuarios para la solicitud, renovación, revocación, etc. de sus certificados digitales.

Los certificados digitales se emiten y revocan mediante resolución del Gerente Municipal a no ser que el usuario lo revoque como consecuencia de alguna incidencia como puede ser la pérdida del certificado. En este sentido, para la emisión de un certificado digital cada área remite a gerencia una solicitud y se emite la resolución de gerencia correspondiente.

Para las bajas, se seguirá el mismo procedimiento. En paralelo se aplicará un control proactivo desde RRHH, en el cual, desde RRHH se comunicará a la Oficina de Registro las bajas de usuarios o cambios de funciones que supongan la revocación del certificado digital.

En cambios del equipo de gobierno se hace una revisión de todos los certificados digitales de los cargos y se revocan los certificados innecesarios y se emiten los adicionales que resulten necesarios.

Finalmente, el Ayuntamiento lleva un inventario de los certificados que dispone. El responsable de dicho inventario es ANIMSA. El inventario de certificados digitales incluye el número de certificado, el tipo de certificado, el emisor del certificado, la persona o aplicación que gestiona el certificado, así como la fecha de caducidad del certificado, entre otros datos.

En el momento en que ANIMSA, detecta que un certificado incluido en el inventario está a punto de caducar (3 meses antes de este hecho), comunica al responsable de dicho certificado, sea este una persona en el caso de certificados de trabajador público o al responsable de la aplicación, en el caso de sellos electrónicos y sede electrónica, de este hecho para que esta persona o responsable pueda iniciar el trámite de renovación del certificado digital siguiendo los procedimientos establecidos.

11.8 Sello de tiempo

Las características principales del sello de tiempo serán:

- El sello de tiempo es una firma electrónica generada por un tercero de confianza en base a un certificado digital especialmente destinado al efecto.
- Evidencia de la fecha y hora en que se ha producido un acto. Se utiliza conjuntamente con un documento en cualquier formato y que puede estar firmado electrónicamente. El sello de tiempo puede hacer referencia a:
 - Firma del documento: el sello de tiempo está asociado a la firma electrónica.
 - Creación del documento: el sello de tiempo está asociado al documento.
- Mediante un proveedor de sellado de tiempo, se sellará la fecha y hora del instante en el que se ha realizado el acto. El proveedor será la @firma TSA.
- Se deberá disponer de un proveedor de sello de tiempo alternativo para garantizar la disponibilidad de los procedimientos de sellado de tiempo. Estos proveedores deben estar sincronizados con una fuente fiable de tiempo como por ejemplo el reloj de la Real Armada Española. Existen diversas fuentes de sellado de tiempo en el mercado, y habrá que escoger las que más convengan dependiendo de: disponibilidad del servicio, calidad del proveedor, coste del servicio, posibilidad de firma de acuerdos de nivel de servicio y autoridad certificada para este servicio.

- El proceso consiste en crear una evidencia electrónica sobre una firma electrónica: se calcula el resumen criptográfico del documento y/o sus firmas electrónicas (en el caso del resellado), es decir, una operación matemática que se aplica al conjunto de información sobre el que emitir el sello de tiempo y obtiene una cadena de bits denominada "hash" la cual se cifra con la clave privada del certificado de sello de tiempo utilizado para hacer la operación. Se retorna esta firma conjuntamente con la fecha y hora de la operación, así como información sobre el certificado de sello de tiempo utilizado para hacer la firma.

11.9 Clases, tipos y niveles de firma.

En este apartado se recopilan los aspectos relacionados con la firma electrónica en el marco del Ayuntamiento, incluyendo los diferentes usos de la firma electrónica en el ámbito de los sistemas del Ayuntamiento. Los objetivos que persigue el Ayuntamiento con la implantación de la firma electrónica son fundamentalmente tres:

- Dotar al Ayuntamiento de un sistema para el control, el uso y la conservación de la documentación original firmada electrónicamente, gestionada en el desarrollo habitual de su actividad política y administrativa.
- Garantizar la gestión adecuada de los documentos del Ayuntamiento, asegurando la autenticidad, la fiabilidad, la integridad y la disponibilidad futura a lo largo de su ciclo de vida, basado en un software informático que ofrece una capa de gestión de documentos y archivo común.
- Dar respuesta a las exigencias en materia de archivo electrónico de la Ley 11/2007, de 22 de junio, y, a partir del 2 de octubre de 2016, la ley 39/2015, de 1 de octubre, y del Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica (Real Decreto 4/2010, de 8 de enero)

Una vez formulados estos objetivos básicos, hay que tener presente la definición de las **clases de firma** desde un punto de vista jurídico:

- **Ordinaria:** es el conjunto de datos en forma electrónica, consignados conjuntamente con otros o que están asociados, que pueden ser utilizados como medio de identificación del firmante (donde identificación debe entenderse como autenticación de entidades, según lo que establece la Directiva 99/93/CE, de 13 de diciembre, de firma electrónica).
- **Firma electrónica avanzada:** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que hace referencia y que ha estado creada por medios que el firmante puede mantener bajo su control exclusivo.

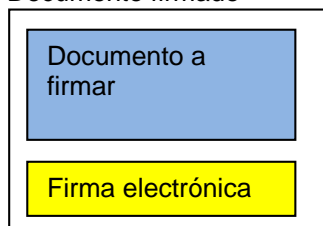
- **Firma electrónica reconocida:** es la firma electrónica avanzada que se basa en un certificado reconocido y que ha estado generada mediante un dispositivo seguro de creación de firma, según establece el artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Para las definiciones anteriores, se utiliza el concepto clave de certificado reconocido, que según la Ley 59/2003, de 19 de diciembre, de firma electrónica, en su artículo 11.1, lo define como aquellos certificados electrónicos emitidos por un prestador de servicios de certificación, que cumplen con los requisitos establecidos en la misma Ley en cuanto a la comprobación de la identidad y el resto de circunstancias de los solicitantes, y la fiabilidad y las garantías de los servicios de certificación que presten.

Definiciones de **tipos de firma** desde un punto de vista técnico:

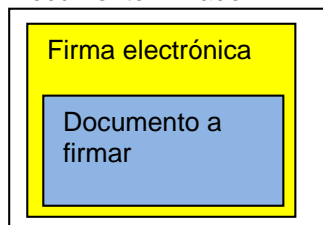
- **Firma attached:** los datos de firma residen en el documento firmado. Por tanto, el mismo documento dispone de toda la información para comprobar la autenticidad e integridad del documento, así como la información necesaria para la validación de la firma. Hay que diferenciar entre dos tipos diferentes de firma attached:
 - Enveloped (incrustada), en este caso el documento firmado está compuesto por el contenido del documento a firmar más la firma de este contenido.

Documento firmado

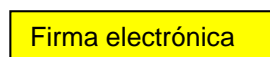
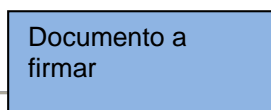


- Enveloping (envolvente), en este caso el documento firmado es la firma electrónica del documento a firmar y dentro de esta firma está el propio documento a firmar.

Documento firmado



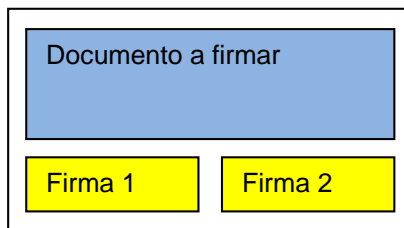
- **Firma detached:** los datos de firma residen fuera del documento a firmar, pero asociados a éste. Los datos de la firma se mantendrán por separado durante todo el ciclo de vida del documento. Para validar la firma hay que crear un documento de evidencia electrónica que contenga de forma conjunta el documento y sus datos completos de la firma.



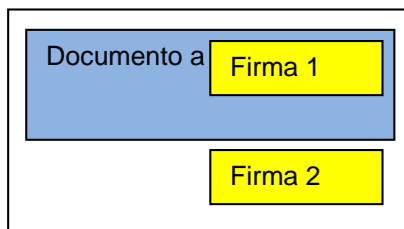
A continuación, definiremos el **nivel de firmas**.

- **Firma simple:** el documento contiene una única firma.
- **Firma múltiple:** el documento contiene dos o más firmas. Esta firma múltiple consiste en que varios firmantes firmen el documento consecutivamente. Esta firma se puede aplicar sobre el documento original cada vez, lo que se identifica como firma **paralela**, o sobre el documento firmado, que se identifica como firma **anidada**.

Documento firmado con firma paralela:



Documento firmado con firma anidada:



La firma múltiple se utilizará en diversas situaciones en el marco de los procedimientos del Ayuntamiento, como por ejemplo en la firma de documentos electrónicos por más de una persona o en el resellado de documentos (ver apartado 11.6) ya firmados para actualizar la validez legal del documento a lo largo del tiempo, antes de que pueda quedar entredicho la validez criptográfica de la firma electrónica.

11.9.1 Formatos de firma

Partiendo de los conceptos básicos sobre firma electrónica descritos anteriormente, a continuación, se describen los formatos de firma electrónica que va a utilizar el Ayuntamiento en el marco de esta política de firma.

11.9.1.1 Firma electrónica con política de firma y con sello de tiempo.

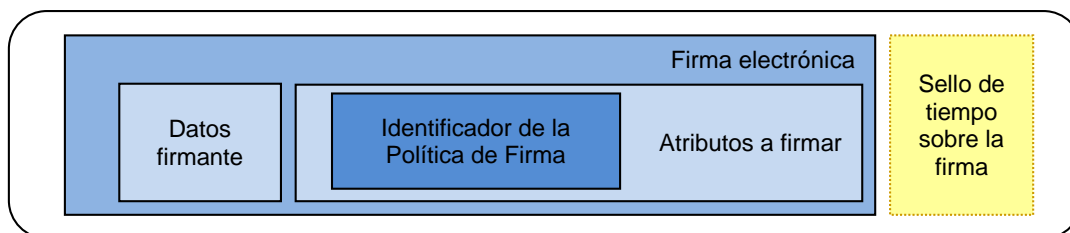
Este será el formato de firma electrónica para los documentos electrónicos y foliados de expediente que se tengan que guardar menos que el tiempo de caducidad del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta:

- En paralelo: primera fecha de caducidad del sello de tiempo dentro de las distintas firmas.
- Anidadas: fecha de caducidad del sello de tiempo de la última firma.

Formato de firma derivado de la firma electrónica avanzada con identificador de política (en nuestra nomenclatura normativa de firma electrónica), también conocida EPES, con la incorporación de un sello de tiempo que sitúa la firma electrónica en un momento determinado del tiempo.

La representación gráfica de este formato de firma, identificado como AdES-T es la siguiente:

AdES-T



La firma electrónica con política explícita (XAdES-T o PAdES-T), debe contener todos los elementos que se listan a continuación de los cuales todos, excepto el último, corresponden al formato XAdES-EPES o PAdES-EPES (firma electrónica avanzada con identificador de política):

- Los datos firmados por el usuario, como por ejemplo un documento electrónico
- El tipo de contenido firmado: ContentType
- El resumen criptográfico del mensaje: MessageDigest
- El certificado empleado para firmar: ESSSigningCertificate o OtherSigningCertificate
- La fecha y hora alegada de la firma: SigningTime (Opcional)
- Las pistas sobre el contenido firmado: ContentHints (Opcional)
- La identificación del contenido: ContentIdentifier (Opcional)
- La referencia a los contenidos: ContentReference (Opcional)

- La indicación del tipo de compromiso: CommitmentTypeIndication (Opcional)
- La localización del firmante: SignerLocation (Opcional)
- Los atributos del firmante: SignerAttributes (Opcional)
- El sello de fecha y hora sobre el contenido: ContentTimestamp (Opcional)
- Contrafirma: Countersignature (Opcional)
- Identificación de la política de firma: SignaturePolicyIdentifier (en nuestra nomenclatura normativa de firma electrónica)
- Sello de fecha y hora de la firma: SignatureTimeStamp

11.9.1.2 Firma electrónica de archivo

Este será el formato de firma electrónica para los documentos electrónicos y foliados de expediente que se tengan que guardar más del tiempo de caducidad del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta:

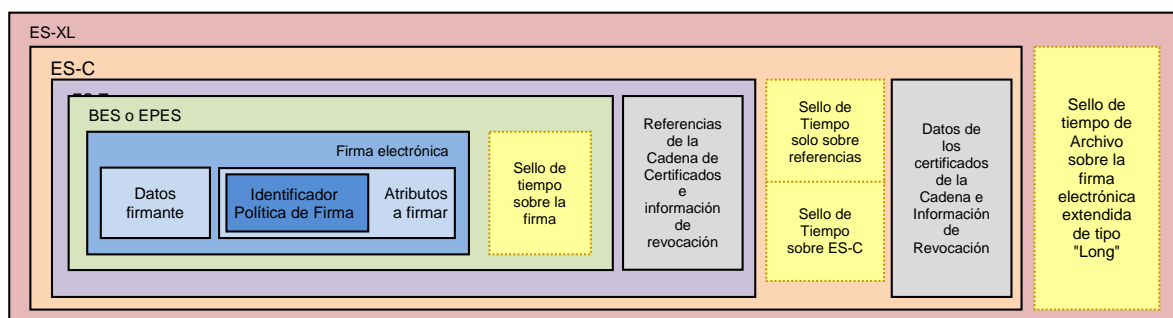
- En paralelo: primera fecha de caducidad del sello de tiempo dentro de las distintas firmas.
- Anidadas: fecha de caducidad del sello de tiempo de la última firma.

Existen dos formatos: AdES-A y PADES-LTV

Firma AdES-A: XAdES-A y CAdES-A

La firma electrónica de archivo (AdES-A) parte del formato de firma electrónica extensa (XL), que incluye todos los elementos de verificación de la vigencia del certificado para poder repetir la validación de manera autónoma. Sobre este formato extenso de firma, añade un sello de tiempo, previendo el resellado sucesivo de manera periódica. Este es el formato de firma más completo y está pensado expresamente para los documentos que se quiere garantizar la disponibilidad a lo largo del tiempo.

Firma electrónica de Archivo (ES-A)



- La firma electrónica XML: Signature
- El certificado utilizado para firmar: SigningCertificate o KeyInfo:X509Data
- La fecha y hora alegada de la firma: SigningTime (Opcional)
- El formato del objeto de datos firmado: DataObjectFormat (Opcional)
- La indicación del tipo de compromiso: CommitmentTypeIndication (Opcional)
- El lugar de producción de la firma: SignatureProductionPlace (Opcional)
- El rol del firmante: SignerRole (Opcional)
- El sello de fecha y hora sobre el contenido: AllDataObjectsTimeStamp o IndividualDataObjectsTimeStamp (Opcional)
- La contrafirma: Reference o CounterSignature (Opcional)
- Identificación de la política de firma: SignaturePolicyIdentifier (en nuestra nomenclatura normativa de firma electrónica)
- Sello de fecha y hora de la firma: SignatureTimeStamp
- Referencias completas de certificados: CompleteCertificateRefs
- Referencias completas de revocación: CompleteRevocationRefs
- Referencias completas de certificados de atributos: AttributeCertificateRefs
- Referencias completas de revocación de atributos: AttributeRevocationRefs
- Sello de fecha y hora sobre la firma completa: SigAndRefsTimeStamp
- Sello de fecha y hora sobre las referencias de certificados y revocaciones: RefsOnlyTimeStamp
- Valores de certificados: CertificateValues
- Valores de revocación: RevocationValues
- Valores de certificados de atributo: AttrAuthoritiesCertsValues
- Valores de revocación de certificados de atributo: AttributeRevocationValues
- Sello de fecha y hora de archivo: ArchiveTimeStamp

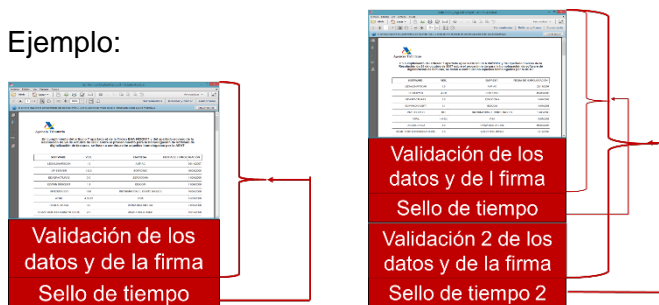
Firma PAdES-LTV

La firma electrónica de larga duración (Long Term Validation) es un formato específico de la familia PAdES. La firma más básica, la PAdES Basic además está especificada en una ISO, la ISO 32000-1. La firma PAdES EPES incluye la firma electrónica del documento (en formato CAdES-BES), con sello de tiempo (recomendado) y una respuesta de validación de un servicio OCSP (recomendado). Puede incluir además motivos de firma, el lugar de la firma y datos de contacto del firmante. Incluye además la política de firma.

Sobre estas firmas se puede construir una firma PAdES-LTV que incluye para la verificación de las firmas y del contenido, de que las Autoridades de Certificación en el momento de la validación eran correctas, la respuesta del servicio de validación OCSP y un sello de tiempo sobre esta verificación de firmas.

Se puede añadir a la firma, posteriormente un nuevo comprobante de verificación que garantiza que la verificación que se hizo en su momento continúa siendo válida y se añade un nuevo sello de tiempo para proteger las firmas y sus validaciones.

Ejemplo:



11.9.2 Validación de firmas

Para garantizar la validez jurídica de los documentos electrónicos firmados digitalmente, cualquier documento que entre o se genere en el Ayuntamiento y que contenga una firma electrónica y/o un sello de tiempo, previamente a su almacenaje en el gestor documental, es necesario validarlo.

Para validarlo se utilizará alguno de estos sistemas:

- Con las herramientas proporcionadas por la compañía KSI (dll's) contra la ruta del servicio OCSP que informa el mismo el certificado digital con el que se ha emitido la firma.
- Con el servicio de validación de PDF que aporta el propio Adobe PDF.
- La plataforma de validación de @firma, y los procedimientos que ésta establezca en cada momento.

Sólo en aquellos casos en que el proceso de validación de todas las firmas electrónicas y de los sellos electrónicos sea satisfactorio se procederá a almacenar el documento electrónico dentro del gestor documental del Ayuntamiento.

En el caso de que sea necesaria la preservación de la validez jurídica del documento más allá del tiempo de vida del certificado digital utilizado para generar cualquier firma asociada a este documento, o del sello de tiempo asociado a la o las firmas electrónicas se procederá a completar la firma o firmas electrónicas en el caso de que estas no sean ya firma de archivo, es decir -A o -LTV. El completado se realizará a formato de firma de archivo.



11.10 Mantenimiento de las firmas

La firma electrónica otorga validez jurídica a los documentos electrónicos. No obstante, esta validez está sujeta a ciertos riesgos que deben gestionarse debidamente para garantizar una validez jurídica indefinida del documento en soporte electrónico. Estos riesgos son:

1. Caducidad del certificado digital con el que se firma un documento electrónico. Puede cuestionarse la validez de un documento electrónico a partir del día que caduque el certificado digital que lo firmó, si no se puede acreditar con total garantía la fecha en que se generó dicha firma, la cual debe ser evidentemente posterior a la fecha de emisión del certificado digital y anterior a la fecha de revocación o caducidad del certificado digital. Para garantizar el momento en que se generó la firma electrónica, ésta puede completarse con un sello de tiempo emitido por una Autoridad de Certificación. En el caso del Ayuntamiento estaremos hablando de realizar firmas AdES-T tanto a nivel de PDFs como de XML.
2. Validez del certificado digital en el momento de generarse la firma electrónica. Puede cuestionarse la validez de un documento electrónico si no existe evidencia suficiente de que el certificado digital estaba vigente el día que se generó la firma electrónica, es decir, no estaba revocado. Para guardar la evidencia de que un certificado digital en una fecha determinada, la de la firma, no estaba revocado puede completarse la firma con la información de la validación de este aspecto contra la Autoridad de Certificación emisora del certificado en el momento emisión de la firma. En este sentido hay que tener en cuenta que las autoridades de certificación, en el momento en que un certificado digital caduca, eliminan las evidencias de revocación de su lista de revocados por lo que si no se guarda la evidencia mencionada una vez caducado el certificado no existirá la certeza de que el certificado con el que se generó la firma no estaba revocado en el momento de generarla. En el caso del Ayuntamiento para garantizar este caso estaremos hablando de firmas AdES-XL o superiores (AdES-A o PAdES-LTV)
3. Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital y con las que se generan las firmas electrónicas. Un documento electrónico puede dejar de tener validez jurídica a partir del día en que se ponga en duda la seguridad de las claves criptográficas con las que se firmó. En este escenario podrían reproducirse de forma incontrolada firmas generadas con las claves puestas en duda y, por lo tanto, todas las firmas generadas con la tecnología obsoleta se pondrían en duda. Para resolver este aspecto se requiere de claves criptográficas de mayor longitud y generar sucesivos refirmas a partir de firmas que permitan incorporar estos sellos de tiempo. En el caso del Ayuntamiento (AdES-A o PAdES-LTV)

11.10.1 Resellado de firmas electrónicas

El objetivo principal de esta función es garantizar la firma electrónica a lo largo del tiempo.

El proceso de resellado consiste en renovar el sello de fecha y hora, añadiendo un nuevo eslabón a la cadena de evidencias electrónicas a la firma electrónica que ya está en el documento.

Para poder aplicar dicho proceso es necesario que las firmas estén en un formato que permita añadir dichas evidencias de tiempo. Estas son las firmas del tipo XAdES-A, CAdES-A o PAdES-LTV. En el caso de que una firma no esté en estos formatos, previo al resellado deberemos completar la firma, que en cualquier caso estará como mínimo en un formato AdES-T a uno de los formatos anteriormente definidos.

Este será un proceso que se llevará a término:

- En el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar.
- Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves utilizadas para firmar el documento.

Partiremos, tal y como se ha comentado en el punto anterior del supuesto de que los documentos tendrán ya una firma del tipo longevo: XAdES-A o PAdES-LTV. Sobre estas firmas se incorporará un nuevo sello de tiempo, puesto que su estructura permite dicha posibilidad. Este nuevo sello de tiempo, estará ya generado con un certificado reciente, con un período de validez superior al actual en la firma a resellar, con una longitud de clave que no estará comprometida y con un algoritmo que no esté sujeto a la obsolescencia criptográfica del algoritmo en el momento de su emisión.

En definitiva, el resellado consiste, pues, en mantener la validez de la firma incorporando nuevo material criptográfico, concretamente sellos de fecha y hora, en la misma estructura de la firma electrónica.

11.10.2 Mantenimiento de la validez jurídica de las firmas en fase de vigencia

El proceso de mantenimiento de las firmas electrónicas en el Ayuntamiento será el siguiente, para el caso de aquellos documentos que deban guardarse más allá de la validez del sello de tiempo incorporado a la firma electrónica de este:

1. En el caso de firmas generadas dentro del entorno del Ayuntamiento, es decir que las firmas se hayan generado mediante las herramientas de firma de este, se procederá en fase de tramitación a la generación de las firmas electrónicas ya en formato preservable, es decir en formato de firma de archivo, para documentos XML las firmas se transformarán a XAdES-A, como podría ser el caso del foliado del expediente, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.

2. En el caso de firmas que provienen de plataformas externas: otras administraciones, herramientas de cliente, etc. se procederá en su caso a completarlas hasta un formato preservable. Dicho proceso de completación se realizará previo cierre y foliado del expediente. Para documentos XML las firmas se pasarán a XAdES-A, como podría ser el caso del foliado del expediente, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.
3. En el caso de que no sea posible generar para algún documento una firma preservable, se procederá lo antes posible a foliar el expediente con un XML con una firma XAdES-A, de forma que sea el foliado del expediente el que garantice la validez jurídica de la firma electrónica del documento.

11.11 Metadatos de firma.

Los Metadatos de firma que utilizará el Ayuntamiento son los siguientes:

ELEMENTOS (EEMGDE17 - FIRMA)

Código	Nombre	Definición	Obligatorio ENI	Obligatorio Ayuntamiento
eEMGDE17.1	Tipo de Firma	Tipo de firma indica si es firma electrónica ordinaria, avanzada o reconocida	SI	SI
eEMGDE17.2	Formato de Firma	El formato de firma indicará si la firma es un XAdES o un PAdES y su nivel de completitud: T, A o LTV		SI
eEMGDE17.3	Rol de Firma	Identifica la normativa de firma aplicada sobre la acción de firmar		SI
eEMGDE17.4	Firmante	DNI o NIF del firmante		SI

Existen otros metadatos que será importante tener en cuenta posteriormente

Código	Nombre	Definición	Obligatorio ENI	Obligatorio Ayuntamiento
eEMGDE17.5	Nombre del firmante	Nombre del firmante o del organismo en el caso de sellos electrónicos		
eEMGDE17.6	Fecha de Firma	Fecha de creación de firma		
eEMGDE17.7	Fecha última verificación de Firma	Fecha de la última verificación de la firma		
eEMGDE17.8	Organismo firmante	Nombre del organismo al que pertenece el certificado en el		

		caso de trabajador público o empresa		
eEMGDE17.9	Modalidad de firma	Valores: Envolvente (Attached - Enveloping) Incrustada (Attached-Enveloped) Independiente (Detached)		

11.12 Casos de uso de la firma electrónica.

Previo a la descripción de los casos de uso identificados de firma electrónica, es interesante comentar un concepto clave en este entorno de la documentación administrativa, y que no es otro que el expediente electrónico y su foliado electrónico. Para ello se aprovecha la definición que hace la Ley 39/2015, en su artículo 70:

- Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.
- Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad, y se enviará completo, foliado, autenticado y acompañado de un índice, asimismo autenticado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

La estructura del foliado del expediente electrónico deberá contener los metadatos del expediente y la lista exhaustiva de todos los documentos que formen parte del expediente (Artículo 32.1 de la Ley 11/2007 y artículo 70.3 de la ley 39/2015 a partir del 2 de octubre de 2016), y para cada uno de los documentos se guardará:

- Clave del catálogo (identificador del documento dentro del expediente).
- Nombre del fichero.
- Resumen/Hash del documento.

Finalmente, el índice del contenido del expediente, se guardará en un fichero XML, que deberá estar firmado con sello electrónico del Ayuntamiento. Esta firma será en formato XML, y más concretamente firma XAdES-A. Después de definir los conceptos de expediente electrónico y de foliado del mismo, se describen los escenarios identificados:

11.12.1 Firma electrónica de un documento electrónico

Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida, ya sean documentos creados o generados electrónicamente por otras aplicaciones.

Las principales características de este escenario son:

- Se realiza la firma sobre un documento original en soporte electrónico.
- El documento original y las firmas se deben incorporar al sistema.
- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla y completarla, utilizando un servicio o autoridad de validación.
- Hay que incorporar al sistema, la evidencia de validación, que en nuestro caso será la firma completada, la cual será en el caso de XML el mismo documento con firma attached y en el caso de PDFs el mismo documento también con firma attached. Es decir no vamos a gestionar firmas detached.
- El documento electrónico estará en cualquier formato de los aceptados por el Ayuntamiento, preferiblemente PDF y XML, siempre que sea necesario garantizar su preservación a lo largo del tiempo.
- El documento se podrá firmar diversas veces y por diferentes usuarios.
- Se podrá firmar en paralelo y/o de forma anidada.
- En el caso de documentos que no se deban guardar más allá de la validez del sello de tiempo que utilice el Ayuntamiento, la firma se generará en formato AdES-T o si no es posible, se completará a este formato.
- En el caso de que los documentos se deban guardar más allá de la validez del sello de tiempo que utilice el Ayuntamiento, la firma electrónica se generará o se completará a AdES-A. Para los documentos PDF será PDF-LTV y para los documentos XML será XAdES-A.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- Clase de firma: Avanzada o Reconocida.
- Tipo de certificado: Para las firmas generadas por el Ayuntamiento: Certificado de trabajador Público o Certificado de Sello Electrónico de Camerfirma. Para las firmas generadas por los ciudadanos: estudiantes, empresas, personas físicas, etc. Cualquier certificado definido en el punto 4.2 del presente documento.
- Formatos: PAdES. Inicialmente en formato PAdES-T. En el caso de preservación se completará la firma a formato PAdES-LTV.
- Sello de tiempo: Sí

- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.
- Normativa de firma: Acto administrativo genérico.

11.12.2 Copia auténtica electrónica de documentos en papel: digitalización segura.

Permite obtener documentos electrónicos con consideración de copia auténtica a partir de documentos en soporte papel.

Las principales características de este escenario son:

- Consiste en la firma electrónica de un documento digitalizado, en formato PDF, para crear una copia auténtica electrónica.
- La firma es necesaria para garantizar la integridad y la autenticidad del documento digitalizado, así como la fecha de dicha digitalización.
- El personal del Ayuntamiento que digitaliza la documentación es el responsable de firmar electrónicamente el documento digitalizado, y debe estar habilitado para hacerlo.
- Los documentos digitalizados se firman incorporando un sello de tiempo. Se genera una firma PAdES-T
- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla.
- En el caso de que los documentos se deban guardar más allá de la validez del sello de tiempo que utilice el Ayuntamiento, la firma electrónica se generará o se completará a PAdES-A.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada
- Tipo de certificado: Certificado de trabajador Público o Certificado de Sello Electrónico de Camerfirma.
- Formatos: PAdES. Inicialmente en formato PAdES-T. En el caso de preservación se completará la firma a formato PAdES-LTV.
- Sello de tiempo: Sí
- Nivel de firma: Simple
- Tipo de firma: Attached.
- Normativa de firma: Compulsa electrónica.

11.12.3 Copia auténtica electrónica de un documento firmado electrónicamente

Permite obtener copias electrónicas de documentos originales firmados electrónicamente aplicando un cambio de formato a PDF para entregar al ciudadano o a otras Administraciones. Este sería el caso de generación de un documento electrónico como copia auténtica de otro documento electrónico en el que se incorpora un código seguro de verificación (CSV) de forma que se pueda imprimir y posteriormente, y mediante este CSV, comprobar en la sede electrónica que dicho documento impreso no se ha manipulado.

Las principales características de este escenario son:

- A partir de un documento original firmado electrónicamente se obtiene una copia auténtica (por ejemplo, en PDF), firmada digitalmente, para entregarla al interesado.
- La copia del documento electrónico deberá estar en un formato normalizado y estandarizado, antes de firmarla.
- El documento se firmará automatizadamente una única vez con sello de órgano, según establece la Ley 11/2007 en su artículo 30.5 y, a partir del 2 de octubre de 2016, el artículo 27 de la ley 39/2015 y artículo 42 de la ley 40/2015: “las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad por medio del acceso a los archivos electrónicos” del Ayuntamiento y en el artículo 18.1.a) de la ley 11/2007: “Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúne los requisitos exigidos por la legislación de firma electrónica. ”A partir del 2 de octubre de 2016, la referencia a la definición del sello electrónico se encontrará en el artículo 42.a) de la ley 40:2015: “Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.”
- Este documento, normalmente en formato PDF, que se entregará al ciudadano en soporte papel, incluirá una URL única que referencia al documento original.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada.
- Tipo de certificado: Certificado de Sello Electrónico de Camerfirma.
- Formatos: Firma en PDF. Se generará en formato PAdES-T. En el caso de que este documento se deba conservar en los expedientes del Ayuntamiento, se procederá a completar la firma, creando un PAdES-LTV.
- Sello de tiempo: Sí

- Nivel de firma: Simple
- Tipo de firma: Attached.
- Normativa de firma: Copia Auténtica Documento Firmado Electrónicamente.

11.12.4 Procesos de firma automatizada

Permite la firma de diversos documentos de forma automática con garantías jurídicas. No requiere la intervención del firmante en el proceso de firma ya que sólo puede ser realizada con certificados de sello electrónico.

Las principales características de este escenario son:

- Firma de diversos documentos de forma automática.
- El documento electrónico podrá estar en cualquier formato de los aceptados (PDF y XML).
- Se guardará en el repositorio seguro del servidor del Ayuntamiento, tanto los certificados digitales como sus correspondientes claves públicas que deben permitir generar procesos de firma automatizada.

Una vez descritas las características concretas de este escenario, se enumeran los criterios de aplicación y actuación:

- Este escenario está pensado para aquellas tareas en las que se deben firmar diversos documentos de forma automatizada con garantías jurídicas.
- Se utilizará un certificado de sello electrónico o de órgano, que firmará los documentos en nombre de la aplicación y del Ayuntamiento.
- Existirá una evidencia de que el responsable del certificado guardado en el repositorio seguro del Ayuntamiento, ha autorizado la firma automatizada.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada para los certificados de sello electrónico o de órgano que son avanzados.
- Tipo de certificado: Certificado de Sello Electrónico de Camerfirma.
- Formatos: Para documentos XML: XAdES-T y para su conservación, XAdES-A. Para documentos PDF: PAdES-T y para su conservación PAdES-LTV.
- Sello de tiempo: Sí
- Nivel de firma: Simple
- Tipo de firma: Attached.
- Normativa de firma: Firma automatizada.

Este es un escenario que abarca diversos ámbitos que se podrían llegar a identificar como subescenarios diferentes, como pueden ser:

- Firma automatizada en procesos de digitalización masiva.
- Resellado de documentos para actualizar su validez criptográfica.
- Para procedimientos de intercambio de información entre administraciones.

11.12.5 Incorporación de documentos firmados digitalmente por parte del ciudadano.

En el caso en el que el ciudadano entregue un documento firmado electrónicamente por él, será necesario:

- Validar las firmas electrónicas del documento.
- En el caso de que las firmas no sean AdES-T o AdES-A/LTV se procederá a completarlas hasta uno de estos niveles en función del tiempo que se deba guardar el documento.
- A continuación, se procederá a incorporar al sistema, el documento con sus firmas completadas.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

- Tipo de firma: Avanzada o Reconocida en función de los certificados utilizados para su firma.
- Tipo de certificado: Cualquier certificado definido en el punto 4.2 del presente documento.
- Formatos: Para documentos XML: XAdES-T y para su conservación, XAdES-A. Para documentos PDF: PAdES-T y para su conservación PAdES-LTV.
- Sello de tiempo: Aconsejado. Una vez completada la firma: Sí
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.
- Normativa de firma: Acto administrativo genérico.

12. Glosario de terminología

Con la finalidad de propiciar el uso de un lenguaje común que favorezca el trabajo pluridisciplinar de todos los sectores implicados en el gobierno electrónico, es necesario definir la terminología utilizada usualmente en el ámbito de la gestión de los documentos y archivos. Dada la importancia de la homologación y la estandarización de los términos que se utilicen, es necesario buscar una suerte de lengua franca que facilite el trabajo conjunto y coordinado de todos los actores y, muy especialmente, de los dos sectores claves: los tecnólogos y lo archivistas o gestores de documentos.

La irrupción constante de conceptos –información, datos, documentos- obliga a una cierta clarificación para verificar el carácter unívoco de cada denominación. En todo caso, existe un notable consenso en el hecho que los datos, combinados entre sí, y mediante la aplicación de un proceso interpretativo pueden dar lugar a una información que, a su vez, para tener sentido, debe ser fijada de manera estable y perdurable en un documento.

- **Acceso:** posibilidad de los ciudadanos de hacer efectivo el derecho democrático de acceso a la información de las administraciones públicas de acuerdo con la legislación vigente.
- **Ciclo vital de los documentos:** cada una de las etapas por las que sucesivamente pasan los documentos que se generan en las oficinas hasta que son eliminados o bien transferidos para su conservación en un servicio de archivo.
- **Clasificación de los documentos:** función archivística intelectual que fundada en el principio de respeto al origen y procedencia y en el principio de respeto al orden origina, consiste en el establecimiento de las categorías y grupos que reflejan la estructura administrativa y funcional del organismo productor de un fondo documental.
- **Conversión:** proceso de transformación de un documento u otro objeto digital de un formato, o versión de formato, a otro.
- **Descripción:** proceso integrante del tratamiento archivístico que implica la elaboración de diferentes niveles de instrumentos de información de los fondos documentos y sus metadatos, para facilitar su conocimiento, acceso y difusión.
- **Documento:** entidad de información de carácter único, producido o recibido en el inicio, desarrollo o finalización de una actividad, el contenido de la cual, estructurado y contextualizado, se presenta como evidencia y soporte de las acciones, decisiones y funciones propias de las organizaciones y de las personas físicas y jurídicas. La información de un documento puede concretarse en cualquier tipo de soporte (papel y electrónico, fundamentalmente).

Usualmente, en las leyes de archivo se precisa que un documento es toda expresión en lenguaje oral, escrito, de imágenes o de sonidos, natural o codificado, recogida en cualquier tipo de soporte material, y cualquier otra expresión gráfica

que constituya un testimonio de las funciones y las actividades sociales del hombre y de los grupos humanos, con exclusión de las obras de investigación o creación.

- **Digitalización:** proceso tecnológico que permite la obtención de uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra de un documento papel a través de técnicas fotoeléctricas de escaneado.
- **Documento administrativo:** documento vinculado al ejercicio de potestades y competencias de las Administraciones Públicas que pueden constituir elemento probatorio de derechos y obligaciones, normalmente generados o aportados en el marco de procedimientos administrativos que sirven como información, conocimiento y testimonio (función de constancia y función de comunicación).
- **Documento de archivo:** unidad de información, registrada en cualquier soporte como evidencia de acciones, producida por un agente en el ejercicio de sus funciones y gestionada por su valor testimonial e informativo.
- **Documento electrónico:** el documento generado, gestionado, conservado y transmitido por medios electrónicos, informáticos o telemáticos, siempre que incorpore datos firmados electrónicamente.
- **Evidencia:** es información ubicada en un contenedor considerado válido y auténtico por la razón que puede demostrarse que no ha sido alterado, que su origen y condiciones de creación es el que se afirma que es y no otros. El contenedor de las evidencias digitales es el documento electrónico.
- **Expediente:** unidad organizada de documentos reunidos bien por su productor para el uso corriente, bien durante el proceso de organización archivística, dado que se refieren al mismo tema, actividad o gestión. La sucesión de expedientes referidos a una misma actividad o función conforman una serie documental.
- **Expediente electrónico:** conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.
- **Expediente híbrido:** conjunto de documentos electrónicos y en papel, tramitados de acuerdo a un mismo procedimiento, relacionados entre ellos.
- **Dato:** unidad básica de información que está dispuesta de manera adecuada para su tratamiento por una computadora. También puede definirse como una representación de hechos, conceptos e instrucciones de una manera formalizada y adecuada para la comunicación, interpretación o procesamiento por medios automáticos o humanos.
- **Dossier:** recogida de información, mayoritariamente de copias organizadas temáticamente, que sirven de complemento a la información contenida en los expedientes administrativos. Los dossiers no tienen validez jurídico-legal y se utilizan como un medio de mera consulta.

- **Firma electrónica:** conjunto de datos en forma electrónica, consignados junto a otros o asociados a ellos, que pueden ser utilizados como medio de identificación del firmante.
- **Formato:** conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.
- **Información:** la información de archivo acredita tres condiciones ineludibles y permanentes; es una información corporativa producida por personas físicas o jurídicas en el desarrollo de sus actividades; es una información previsible en la medida que es el resultado de un proceso preestablecido; y es una información reglada en su producción, uso y conservación mediante normas legales o de procedimiento. En todos los casos, la información es inseparable del soporte que la contiene.
- **Metadato:** dato que define y describe otros datos presentes o asociados en cualquier documento electrónico y permite su localización, inteligibilidad y uso. Existen diferentes tipos de metadatos según su aplicación (descripción, preservación, valoración...).
- **Serie documental:** conjunto de documentos orgánicamente y funcionalmente relacionados, establecido conforme al principio de procedencia, con especial atención a la historia administrativa, la estructura y la calidad de los documentos de oficina, institución u organización implicada.
- **Soporte:** objeto sobre el que es posible grabar y recuperar datos.
- **Tipología:** tipo o género de los documentos de una unidad de descripción (instancia, acta, certificado...).
- **Transferencia:** acto por el cual la conservación de documentos de archivo de una organización es transferida de pleno derecho a un servicio de archivo.
- **Valoración de documentos:** función básica destinada a determinar la clarificación posible de los documentos según sus usos administrativos, fiscales y legales, jurídicos, tanto presentes como futuros, y sus valores testimoniales, informativos y de investigación.

13. Anexo I. Cuestionarios para el análisis de procedimientos

Cuestionario para el análisis del flujo

Información requerida del procedimiento	Comentarios
Diagrama de Flujo del procedimiento	Si existe
Descripción del flujo (p.ej. en normativa interna)	Alternativamente
Descripción del flujo a partir de entrevistas	Alternativamente
Análisis Información - preguntas a responder	Comentarios
¿Cuáles son los agentes que actúan en el procedimiento?	Confirmar que se consideran todos (mediante entrevistas)
¿Cuáles son las dependencias con agentes externos?	Otras instituciones, normativas o convenios
¿Qué validaciones o denegaciones afectan al flujo del procedimiento? ¿Y quién tiene la potestad para realizarlo?	Ampliado en la sección de análisis de roles
¿Existe alguna política/normativa (interna) que afecte al procedimiento?	Define algún paso o todo el procedimiento
¿Cuáles son los plazos establecidos?	Temporalizar el procedimiento
¿Cuáles son las tareas a realizar durante el procedimiento?	Lista de tareas
¿Qué dependencias existen entre las tareas?	
¿Existen tareas superfluas? ¿Y paralelizables?	Optimizar procedimiento
¿Existen tareas que puedan modificarse para mejorar su eficiencia?	
¿Qué leyes regulan el procedimiento?	Aspectos clave que nos permite para su tratamiento digital (p.ej. declaraciones responsables que limiten la documentación a aportar en el inicio del trámite)
¿Qué notificaciones se generan durante el procedimiento?	Documentos a enviar al ciudadano
¿Se requiere de alguna resolución oficial para continuar con el procedimiento? ¿Interna o externa?	
¿Es necesario añadir alguna tarea al procedimiento?	Experiencia/entrevistas
¿Puede eliminarse alguna tarea del procedimiento?	Experiencia/entrevistas
Obtención de resultados	Comentarios
Propuestas de optimización	
Identificación de documentos y agentes relevantes	Para iniciar los dos cuestionarios siguientes
Diagrama de flujo del procedimiento	Si no existe
Documento descriptivo del flujo del procedimiento	Documentación

Cuestionario para el análisis de los roles

Agentes / actores que participan en el procedimiento	Comentarios
Lista de agentes/actores que realizan las tareas	Si existe
Enumerar agentes/actores (a partir de entrevistas)	Alternativamente
Documentación legal relevante de los diferentes roles respecto al procedimiento	Recopilar
Descripción de roles	Si existe
Análisis Información - preguntas a responder	Comentarios
¿Cómo se identifican/autentican los agentes/actores?	Si se realiza telemáticamente
¿Cuál es su rol?	Descripción
¿Qué responsabilidades incorpora este rol?	Posibles acciones a realizar
¿Unipersonal?	
¿En el caso que sólo pueda hacerlo una persona, existe alguna política establecida para cuando está ausente (baja/vacaciones)?	
¿Existe algún conflicto de intereses / necesidad de segregar funciones?	
¿Se requiere certificado digital? ¿De qué tipo?	Personal/Representante empresa con poderes/sin poderes... (tanto internos como externos)
¿Uso de certificados para tareas automáticas?	Infraestructura implantada, si existe.
¿La política de certificación, regula todos los aspectos relacionados con el ciclo de vida de los certificados?	Si existe
¿Cómo se gestionan los certificados digitales?	Alta, baja, renovación, ...
¿La política de gestión de llaves regula su gestión?	Si existe
Obtención de resultados	Comentarios
Lista de agentes/actores y ficha descriptiva para cada rol	
Propuestas para la redacción de normativas de certificación y gestión de las llaves	
Propuestas de definición de roles y tareas asignadas (responsabilidades)	

Cuestionario para el análisis de los documentos

Documentos asociados al procedimiento	Comentarios
Lista de documentos incluidos en todo el procedimiento	Si existe
Plantillas documentales	Si existen
Enumerar los diferentes documentos que participan en el procedimiento (a partir de entrevistas)	Alternativamente
Análisis información - preguntas a responder para cada documento	Comentarios
¿Para qué se requiere? ¿Existen alternativas?	Definir la función del documento en el procedimiento
¿Quién aporta el documento? ¿Quién lo emite?	
¿Es posible obtener el documento o la información que contiene por otras vías?	
¿Cuál es el formato del documento? ¿Se restringen los formatos aceptados?	Formatos aceptados
¿Se requiere de firma? ¿De quién y por qué motivos?	
¿Se digitaliza el documento para facilitar su gestión?	No se requiere copia auténtica
¿Se digitaliza el documento para facilitar su preservación? ¿Es el original un documento ya digitalizado?	Copia auténtica
¿Cómo se guardan los documentos electrónicos firmados?	
¿Los documentos firmados incorporan sello de tiempo?	Para garantizar el momento concreto de la existencia del documento
¿Cuál es la política de archivo de documentos?	Tablas de evaluación documental, transferencia, etc.
Obtención de resultados	Comentarios
Lista de documentos y ficha descriptiva para cada uno	
Propuesta de formatos aceptados	Se recomienda limitar el número de formatos aceptados
Propuesta de política de firma	
Propuesta de redacción de normativa de seguridad documental	

14. Anexo II: Proyecto de digitalización

La digitalización se debe abordar como un proyecto completo el ciclo vital del que abarque las siguientes fases:

- **Actividades previas al proyecto**, incluyendo la identificación de objetivos y metodologías, los recursos y los mecanismos de habilitación.
- **Implementación técnica del proyecto**, donde se realiza el proceso tecnológico de la digitalización y se invierte el mayor esfuerzo.
- **Actividades posteriores al proyecto**, principalmente asociadas con el establecimiento de las responsabilidades de mantenimiento y conservación de los documentos digitalizados.

Como todo proyecto, será necesario incorporar un mecanismo de mejora continua que permita refinar el proceso de digitalización y evitar que se repitan aquellos errores o problemas que hayan podido surgir.

1. Actividades previas al proceso

1.1 Identificación de la motivación de la digitalización

Un proyecto de digitalización puede estar motivado por diferentes razones, entre las que pueden destacarse las siguientes:

- Dar cobertura a la gestión documental electrónica del Ayuntamiento y la cohesión con el documento y expediente electrónico administrativo.
- Generar copias digitales de documentos en papel de tal forma que la copia se convierta copia auténtica y pueda sustituir al documento en soporte papel, permitiendo incluso su eliminación.
- Dar cumplimiento a los requisitos legales establecidos sobre Administración Electrónica en materia de acceso y consulta del ciudadano a la documentación en calidad de interesado que obre en poder de la Administración.
- Facilitar el acceso a la documentación por parte de los usuarios.
- Proporcionar nuevas vías de acceso y uso de la documentación.
- Preservación de los documentos originales frágiles y / o quebradizos la manipulación de los que puede deteriorarlos.

La identificación del principal motivo para digitalizar la documentación en soporte papel es la base de la definición de todo proyecto de digitalización.

1.2 Definición de los criterios de selección

Independientemente de la motivación de la digitalización, la selección de la documentación a digitalizar deberá basarse principalmente en su contenido, es decir, en la justificación de que el esfuerzo invertido en digitalizar el documento aporte valor al Ayuntamiento.

Por lo tanto todo proyecto de digitalización debería tener sus propios principios de valor basados en la motivación y los objetivos que intenta conseguir. Para la definición de estos principios, se puede tener en cuenta los siguientes aspectos:

- Cumplimiento del derecho de comunicación del ciudadano con la administración por medios electrónicos;
- El valor de la serie documental;
- La propiedad intelectual;
- La preservación;
- La viabilidad técnica;
- El desarrollo de la serie documental.

1.3 Definición de los requisitos del proceso

En función de la serie documental seleccionada y la motivación de la digitalización, es necesario definir los requisitos del proceso de digitalización.

- A nivel **procedimental**, definiendo la conformidad con las políticas de gestión documental existentes y estableciendo los procedimientos necesarios.
- A nivel de **agentes implicados**, describiendo los roles y responsabilidades de cada uno.
- A nivel **técnico**, identificando el dispositivo de captura que se ajuste mejor a las características físicas de la serie documental y el software de digitalización más idóneo.
- A nivel **jurídico**, analizando las cuestiones legales que sean aplicables en función del contenido de la serie documental.
- A nivel de **seguridad**, adoptando las medidas oportunas que provean la seguridad proporcional al valor de la serie documental.

1.4 Planificación y documentación del proyecto

Una vez definidos los motivos, objetivos, alcance y requisitos del proceso, se debe elaborar un plan de proyecto que incluya, al menos:

- Definición del alcance, con una identificación clara de la motivación, objetivos, escala, tamaño y límites del proyecto;
- Finalidad y usos previstos de los documentos digitalizados;
- Enumeración e identificación clara de los beneficios que se esperan obtener;
- Enumeración de las necesidades del usuario final;
- Enumeración de las normas técnicas adoptadas, incluidos el formato, la comprensión y los metadatos;

- Equipo y recursos que se utilizarán para la digitalización;
- Procesos para la planificación, el control y la ejecución de la digitalización;
- Procesos de control de calidad;
- Estrategias para integrar la imagen digitalizada en procesos de trabajo;
- Estrategias para la gestión continua de los documentos digitalizados y los documentos originales durante el tiempo que haga falta mantenerlos;
- Estrategias relativas a los requisitos legales para la digitalización de los tipos documentales en cuestión.

2. Implementación técnica

En función del método de digitalización que sea necesario (tradicional o seguro) se realizará el proceso técnico de digitalización formado por las siguientes actuaciones secuenciales:

1. Selección de parámetros.
2. Digitalización por medios fotoeléctricos.
3. Optimización de la imagen electrónica.
4. Creación del documento electrónico.
5. Metadatos.
6. Firma.
7. Captura del documento.

3. Actividades posteriores al proceso

Una vez creados y capturados, los documentos electrónicos digitalizados deben cumplir las condiciones para la recuperación y conservación de cualquier documento electrónico tal como establece el artículo 21 del RD 4/2010 ENI.

Estos documentos electrónicos estarán bajo el amparo de la Política de Gestión de Documentos electrónicos del Ayuntamiento y como tal, se tendrán en cuenta los siguientes aspectos:

- Conservación de la documentación original y digitalizada.
- Destrucción de originales.
- Inserción en expedientes híbridos.
- Mantenimiento y acceso a largo plazo.

15. Anexo III: Requerimientos técnicos mínimos que debe tener un hardware y software para una digitalización segura de documentos electrónicos.

En este anexo se definen los requerimientos mínimos que deben cumplir el software y hardware que se utilicen en los procesos de digitalización segura en los diferentes pilotos.

1 Requisitos de los dispositivos de captura de imagen

El proceso de obtención de una imagen electrónica a partir de un documento en soporte papel puede realizarse por medio de diversos dispositivos de captura de imágenes, como escáneres planos, escáneres para diapositivas, cámaras fotográficas digitales, etc.

Para la digitalización segura de documentos se emplearán dos tipos de dispositivos, escáneres y cámaras fotográficas digitales, para los que se establecerán unos requisitos mínimos técnicos.

1.1 Escáner

Un escáner es un dispositivo de digitalización que, mediante un **barrido**, produce un mapa de bits que representa la imagen que ha procesado.

Las características básicas que definen un escáner y los valores mínimos a considerar incluyen en la tabla siguiente:

Especificación técnica	Descripción	Valor mínimo
Tipo de escáner	Plano o de sobremesa / de trayectoria / de tambor. Con o sin alimentador automático de hojas. En función del objeto a digitalizar: papel, transparencia, diapositiva, objeto sólido, microfilm.	Determinado por las características físicas del documento original.
Tamaño del original	Valores máximos de las dimensiones físicas de los originales, incluyendo el grosor de los mismos que puede escanear. Por ejemplo: DIN A3, DIN A4, ...	Determinado por las dimensiones físicas del documento original.
Profundidad del bit	Número de bits utilizados para representar cada píxel en una imagen. Determina el número de colores que se pueden representar en una imagen digital.	Escala de grises: 4 bits. Color: 8 bits.
Resolución óptica	El número de píxeles (altura y anchura) que constituye una imagen, expresado normalmente como el número de píxeles por pulgada (ppp) o a veces como puntos por pulgada (dpi).	200 ppp ~ 200 dpi.
Rango dinámico	Rango de diferencia tonal entre la parte más clara y la más oscura de una imagen. Cuanto más alto sea el rango dinámico mayor será el nivel de detalle y matices.	Determinado por el nivel de resolución seleccionado.
Velocidad de barrido	Velocidad de escaneo, normalmente expresada en página por minuto (en color y / o blanco y negro).	Determinado por el tiempo máximo por página para el escaneo.
Formato de salida	Las imágenes digitalizadas se pueden guardar en diferentes formatos: TIFF, PDF, PNG, etc.	Determinado por el formato de salida seleccionado para la imagen electrónica.

Iluminación	Indica el nivel de iluminación de la lente medida en lux / hora y temperatura.	1 a 126 lux / hora Temperatura inferior a 0,5 ° C en relación a la temperatura ambiente.
--------------------	--	---

Requisitos técnicos del escáner.

Adicionalmente, se podrían tener en consideración otros requisitos que, en función de la serie documental a digitalizar, sean imprescindibles. Por ejemplo, si la serie documental se encuentra encuadrada deberá seleccionar un escáner que cuente con la capacidad para escanear este tipo de documentos.

1.2 Cámara fotográfica digital

La cámara fotográfica digital puede emplearse como dispositivo de captura de imagen electrónica en aquellos casos en los que la documentación original que no tenga que entrar en contacto físico con el cristal del escáner o bien no es apta para procesarla a través de un alimentador automático de documentos.

Las características básicas que deben considerarse a la hora de seleccionar una cámara fotográfica digital como medio de captura de imagen y sus valores mínimos indicados en esta tabla:

Especificación técnica	Descripción	Valor mínimo
Sensor	Existen dos tipos de tecnologías utilizadas para los sensores de cámaras digitales: CCD (Charge Coupled Device) CMOS (Complementary Metal Oxide Semiconductor). Ambos están formados por semiconductores de metal-óxido (MOS) y están distribuidos en forma de matriz.	CMOS: 20x13mm o 22x15mm. CCD: 23x15 mm.

Resolución	El número de píxeles (altura y anchura) que constituye una imagen.	3000 x 2000 píxeles.
Formato salida	Las imágenes digitalizadas se pueden guardar en diferentes formatos: TIFF, PDF, PNG, etc.	Determinado por el formato de salida seleccionado para la imagen electrónica.
Balance blancos	Capacidad de ajustar el nivel de brillo del color RGB.	Automático. Manual con 5 ajustes.
Distancia focal objetivo	Indica los grados que la lente de una cámara es capaz de abarcar.	35 mm (ángulo de visión de 63 grados).
Tiempo exposición	Período de tiempo durante el cual está abierto el obturador de la cámara.	Valor máximo de tiempo de exposición: 30 segundos.
Sensibilidad ISO	Cantidad de luz necesaria para capturar la imagen.	ISO 100 hasta 1600. ISO 200 estándar.

Requisitos técnicos de la cámara digital.

2. Requisitos del software de digitalización

Durante la fase de optimización de la imagen electrónica obtenida a través de los dispositivos de captura identificados en el apartado anterior, puede ser preciso emplear un software adicional de digitalización que permita procesar y mejorar la imagen.

En relación al procesamiento de imágenes, se recomienda seguir las pautas recogidas en el informe técnico UNE-ISO / TR 15801 IN.

Las técnicas más comunes utilizadas en los procesos de post-escaneado utilizadas para la mejora de la imagen y que pueden tener un efecto sobre la presentación de salida de la imagen y el tamaño del archivo almacenado son:

- eliminación de sesgos (deskew);
- limpieza de basuras / fondo (despeckle / background cleanup),
- retirada de bordes negros (black border Renovales);
- retirada de formularios (forms Renovales);

- filtros personalizados:
 - ajuste de profundidad de bits;
 - eliminación del moaré (descreen);
 - ajuste de nitidez (Sharp).
- corrección de curvatura cuando se escanean documentos encuadernados.

El uso de estas características debe respetar la geometría del documento original y su proporción garantizando, en cualquier caso, tanto la integridad como la fidelidad de la imagen obtenida. Para la aplicación de estas técnicas, destinadas a proporcionar un resultado de imagen óptimo o a mejorar el rendimiento de un proceso automatizado de captura de documentos, el informe técnico UNE-ISO / TR 15801 IN establece una serie de recomendaciones.

3. Requisitos del sistema de firma electrónica

El sistema de firma electrónica utilizado deberá proporcionar internamente los mecanismos necesarios para implementar la firma electrónica reconocida y su validación, de manera que permita garantizar la identificación, autenticación, integridad y no repudio de los documentos digitalizados.

4. Requisitos de la imagen electrónica

Tal como establece la Guía de aplicación de la NTI de Digitalización de documentos:

Los requisitos de la imagen electrónica resultado de un proceso de digitalización se definen con el objetivo de garantizar que el documento electrónico digitalizado:

i. Sea válido para ser conformado como documento electrónico con las características establecidas en la NTI de Documento Electrónico.

ii. Sea fiel al documento en papel; entendida la condición de fidelidad en términos relativos proporcionales a la naturaleza, características o finalidades del producto de digitalización, garantizando, en cualquier caso, los mínimos establecidos en la NTI de Digitalización de documentos.

Por tanto, los requisitos de la imagen electrónica serán aquellos relacionados con los formatos admitidos para las imágenes electrónicas, las condiciones de fidelidad y el nivel de resolución a aplicar.

Los requerimientos de formato se han incluido en el apartado 7 de la presente política.

4.1 Fidelidad

Tal como establece la Guía de aplicación de la NTI de Digitalización de documentos:

Una imagen fiel, con la integridad suficiente a efectos probatorios, de un documento papel es un conjunto de componentes digitales que representan el contenido y aspecto del documento original, así como las características o metadatos asociados que contribuyen a garantizar la fidelidad de la imagen que, en cualquier caso, vendría avalada por la firma electrónica correspondiente al proceso de digitalización.

Esta característica se debe interpretar de forma proporcional a las exigencias de integridad específicas de cada documento, así como la criticidad del documento, la gestión de riesgos y la aplicación de regulaciones específicas.

El objetivo a perseguir es valorar la fidelidad basándose en el principio de como de bien la imagen electrónica transmite la apariencia y contenido del documento original (detalle, color, tono, textura del papel, legibilidad, etc.).

Por lo tanto, durante el proceso de digitalización será necesario aplicar una serie de controles de calidad para garantizar el cumplimiento de los criterios establecidos:

- Nivel de resolución de acuerdo con el documento original.
- Selección adecuada de los parámetros de los dispositivos de captura de la imagen: profundidad de bits, reproducción tonal, nivel de compresión, formato, etc.
- Respetar la geometría del documento original en tamaño y proporciones.
- No inclusión de caracteres o gráficos que no figuren en el documento original.
- En caso de aplicación de un proceso de optimización de la imagen, asegurar el nivel de fidelidad de la imagen.

4.2 Nivel de resolución

El nivel de resolución en la que se capture una imagen electrónica determinará en gran medida su calidad, así como la profundidad de bits con la que se haya hecho la exploración. Ambos aspectos están limitados por el dispositivo concreto (escáner, cámara digital) que se emplee.

El aumento de la resolución permite capturar detalles más precisos. Sin embargo, en algún punto, una mayor resolución no tendrá como resultado una ganancia evidente en la calidad de la imagen, sino un mayor tamaño de archivo. La clave es determinar la resolución necesaria para capturar todos los detalles importantes que están presentes en el documento fuente.

Sin embargo, el nivel de resolución, para cualquier imagen electrónica, indicado en la NTI de Digitalización de documentos es de **200 ppp**, valor mínimo para garantizar la legibilidad de la imagen.

Sin embargo, esta resolución puede no ser suficiente para determinadas series documentales del Ayuntamiento, las particularidades específicas de las que requieran unos valores superiores.

A continuación, se muestra un ejemplo de cuadro comparativo entre la resolución mínima para el formato TIFF en base a las dimensiones, tipo y profundidad del documento a digitalizar. Se han resaltado aquellos documentos que a priori, serán los originales más frecuentes para ser digitalizados.

DOCUMENTOS ORIGINALES	DPI / FORMATO	PROFUNDIDAD DEL BIT
PÚBLICACIONES PERIÓDICAS Sólo texto, DIN A4.	200 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
PÚBLICACIONES PERIÓDICAS Texto e imagen b / n, DIN A4.	200 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
PÚBLICACIONES PERIÓDICAS Sólo texto, DIN A3.	300 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
PÚBLICACIONES PERIÓDICAS Texto e imagen b / n, DIN A3.	300 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
TEXTO IMPRESO DIN A4.	200 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
TEXTO IMPRESO E IMAGEN DIN A4	250 dpi / TIFF sin comprimir	Color, a 24 bits
MANUSCRITO MONOCROMÁTICO DIN A4.	200 dpi / TIFF sin comprimir	Color, a 24 bits
MANUSCRITO COLOR DIN A4.	300 dpi / TIFF sin comprimir	Color, a 24 bits
FOTOGRAFÍA / OPACOS B / N Medidas: 10x15 cm .; 20x24 cm .; 24x30 cm .; 24x30 cm.	300 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
FOTOGRAFÍA / OPACOS COLOR Medidas: 10x15 cm .; 20x24 cm .; 24x30 cm .; 24x30 cm.	300 dpi / TIFF sin comprimir	Color, a 24 bits
FOTOGRAFÍA / NEGATIVOS Y DIAPOSITIVAS B / N Paso universal de 35 mm.	2.600 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
FOTOGRAFÍA / NEGATIVOS Y DIAPOSITIVAS B / N Formato medio, 4x5.5 cm.	1.800 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
FOTOGRAFÍA / NEGATIVOS Y DIAPOSITIVAS B / N Formato medio, 6x7cm.	1.200 dpi / TIFF sin comprimir	Escala de grises, a 8 bits

DOCUMENTOS ORIGINALES	DPI / FORMATO	PROFUNDIDAD DEL BIT
FOTOGRAFÍA / NEGATIVOS Y DIAPOSITIVAS COLOR Paso universal de 35 mm.	2.600 dpi / TIFF sin comprimir	Color, a 24 bits
FOTOGRAFÍA / NEGATIVOS Y DIAPOSITIVAS COLOR Formato medio, 4x5.5 cm.	1.800 dpi / TIFF sin comprimir	Color, a 24 bits
FOTOGRAFÍA / NEGATIVOS Y DIAPOSITIVAS COLOR Formato medio, 6x7cm.	1.200 dpi / TIFF sin comprimir	Color, a 24 bits
FOTOGRAFÍA / PLACAS Tamaño 10x15 cm.	800 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
FOTOGRAFÍA / PLACAS Tamaño 15x20 cm.	600 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
FOTOGRAFÍA / PLACAS Tamaño 20x25 cm.	500 dpi / TIFF sin comprimir	Escala de grises, a 8 bits
MAPAS, PLANOS Y PERGAMINOS Formatos hasta DIN A4.	250 dpi / TIFF sin comprimir	Color, a 24 bits
MAPAS, PLANOS Y PERGAMINOS Formatos DIN A3 o superior.	300 dpi / JPEG, y malla cuadrículada en formato DIN A4 en TIFF sin comprimir.	Color, a 24 bits

Cuadro comparativo. Torres Freixinet, Luis (2009). "Digitalización del patrimonio documental", en TRIA, Revista Archivística de la Asociación de Archiveros de Andalucía, núm. 15, 2009, p. 241-298.

2. Anexo IV: Requerimientos para la digitalización externalizada

El Ayuntamiento de Pamplona, con carácter previo a la externalización, total o parcial, del servicio de digitalización debe definir de forma clara los objetivos de digitalización a corto, medio y largo plazo, así como:

- Especificar en forma completa los requisitos de imagen, metadatos y derivados;
- Identificar proveedores confiables;
- Evaluar productos y servicios relacionados;
- Adoptar políticas y procedimientos para las diversas funciones externalizadas;
- Definir las responsabilidades institucionales y las de los proveedores.

Existen ventajas y desventajas respecto a la elección de externalizar o capacitar internamente al Ayuntamiento para los esfuerzos de digitalización de imágenes. Incluso cuando se toma la decisión de externalizar hay actividades del proceso de digitalización que puede reservarse el Ayuntamiento como son:

- Captura de los documentos digitalizados;
- Control de la calidad y fidelidad de las imágenes electrónicas;
- Firma de los documentos digitalizados;
- Compleción de los metadatos mínimos obligatorios en los documentos digitalizados.

Si el Ayuntamiento decide externalizar el proceso digitalización o parte del mismo deben tenerse en cuenta que, como entidad del Sector Público, debe ajustar su contratación a la legislación de contratos.

La externalización del servicio de digitalización tiene unas peculiaridades propias que exige que en los pliegos de contratación o el contrato se recojan las condiciones de prestación del servicio que debe seguir el contratista a fin de que el proceso de digitalización se realice de manera segura y con garantías para el Ayuntamiento. El objeto del presente Anexo es recoger modelos de cláusulas contractuales que garanticen la externalización de manera adecuada del servicio de digitalización. Estos modelos de cláusulas podrán ser incluidos en los contratos de prestación de servicios de digitalización.

En este sentido, las cláusulas de los contratos que regulen la externalización del servicio de digitalización de documentos en papel deberán garantizar, al menos, lo siguiente:

- Cumplimiento de la normativa de protección de datos de carácter personal.
- Confidencialidad del tratamiento de datos.
- Propiedad intelectual.
- Cumplimiento de plazos.
- Acuerdo de Nivel de prestación del Servicio.

- Posibilidad o no de subcontratar o ceder a terceros parte del servicio.
- Medidas mínimas según el lugar de prestación del servicio.
- Certificación de la digitalización mediante firma electrónica.
- Penalizaciones.
- Responsabilidad del contratista por daños y perjuicios.
- Garantía.
- Jurisdicción.
- Resolución del contrato.

Se desarrollan a continuación una serie de modelos que podrán ser utilizados para la elaboración de las cláusulas que garanticen los mínimos mencionados anteriormente.

Para el desarrollo de contratos con proveedores de servicios de digitalización partiendo de los modelos que se exponen a continuación deberá considerarse que, como mínimo, los aspectos resaltados en **negrita y cursiva** deberán ser personalizados a criterio del Ayuntamiento.

1. Modelos de cláusulas para regir la digitalización externalizada

1.1 Cumplimiento de la normativa de protección de datos de carácter personal

Este contrato implica el tratamiento de datos de carácter personal por lo que el contratista deberá respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo. El acceso del contratista a datos de carácter personal de cuyo tratamiento es responsable el Ayuntamiento de Pamplona, supone que aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a estos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre.

El Ayuntamiento de Pamplona sólo proporcionará los datos personales al contratista en caso de resultar absolutamente necesario para la prestación e implementación del servicio.

El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento y no los aplicará o utilizará con fin distinto al que figure en dicho contrato ni los comunicará, ni siquiera para su conservación, a otras personas, exceptuando aquello indicado en la cláusula 1.6.

El encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la

tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los Centros de tratamiento, locales, equipos, sistemas y programas.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos al Ayuntamiento de Pamplona, o al encargado de tratamiento que ésta hubiera designado. El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto que pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

En caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán cumplirse los siguientes requisitos:

- a. Que este tratamiento se haya especificado en el contrato firmado por el Ayuntamiento de Pamplona y el contratista.
- b. Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.
- c. Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

El contratista informará a su personal, colaboradores y subcontratistas de las obligaciones relativas al tratamiento automatizado de datos de carácter personal. En estos casos el tercero tendrá también la consideración de encargado del tratamiento.

1.2 Confidencialidad del tratamiento de datos

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente las de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este contrato, ni tampoco ceder a otros ni siquiera a efectos de conservación, sin el previo consentimiento por escrito del Ayuntamiento de Pamplona.

Se considerará información confidencial cualquier información a la que el contratista acceda en virtud del presente contrato, especialmente la información y datos propios del contratista o de los usuarios y beneficiarios del servicio, que con tal carácter se indique, a la que haya accedido durante la ejecución del mismo, así como la documentación.

Se excluye de la categoría de información confidencial:

- Toda aquella que haya de ser revelada de acuerdo con las leyes o con una resolución judicial o acto de autoridad competente.

- Toda aquella que sea de dominio público en el momento de ser revelada, o posteriormente se haga pública o de otra forma pasara a ser de dominio público por causa distinta al incumplimiento de lo aquí dispuesto.

El contratista informará a su personal, colaboradores y subcontratistas de las obligaciones establecidas en el presente contrato de confidencialidad. El contratista pondrá todos los medios a su alcance para que su personal y colaboradores cumplan tales obligaciones.

La duración de las obligaciones de confidencialidad establecidas en el presente contrato será indefinida mientras la misma ostente tal carácter, manteniéndose en vigor con posterioridad a la finalización por cualquier causa, de la relación entre el Ayuntamiento de Pamplona y el contratista.

1.3 Propiedad intelectual

En el proceso seguro de digitalización se garantizarán los derechos de propiedad intelectual afectados poniendo las medidas de seguridad adecuadas que eviten cualquier tipo de vulneración de los mismos.

En ningún caso el contratista mantendrá, instalará o configurará software sin las licencias y los debidos permisos. El contratista garantiza al Ayuntamiento de Pamplona que todo el software y hardware que sea usado para implementar sus funciones es original y no vulnera ninguna ley, derecho o interés de tercero alguno, en especial los referidos a propiedad industrial e intelectual y que cuenta con las correspondientes licencias de uso.

El contratista no podrá hacer uso del nombre, logotipo o cualquier signo distintivo o material que le haya facilitado el Ayuntamiento de Pamplona para el cumplimiento de las obligaciones derivadas del presente contrato fuera de las circunstancias y fines de éste, ni una vez terminada la vigencia del mismo.

1.4 Cumplimiento de plazos

El cumplimiento de los plazos recogidos en este contrato tienen carácter esencial y por ello su incumplimiento podrá dar lugar a penalizaciones en los términos previstos en el apartado referido a las mismas.

En caso de que por causa de fuerza mayor alguna de las partes no pueda cumplir total o parcialmente las obligaciones contraídas, el plazo estipulado para el cumplimiento de las obligaciones de la parte afectada se prorrogará durante un tiempo razonable que no excederá, en ningún caso, del período de tiempo en que la causa de fuerza mayor haya impedido el cumplimiento de las correspondientes obligaciones. Se considerará causa de fuerza mayor las huelgas legales que excedan del ámbito del contratista y la finalización de las que no dependa de la decisión de la misma.

1.5 Acuerdo de Nivel de prestación del Servicio

El servicio será realizado de acuerdo con las prescripciones técnicas previstas y la oferta presentada y de acuerdo con las instrucciones relativas a la identificación de los documentos y calidad de la digitalización establecidos por el Ayuntamiento.

El proceso de digitalización debe cumplir con los requisitos establecidos en el modelo de digitalización del Ayuntamiento de Pamplona sujeto a la política de gestión documental del Ayuntamiento aprobada según (en este punto se deberá incluir la referencia a la normativa de aprobación formal del PDDE). Este modelo establece los requisitos técnicos y los niveles mínimos de calidad del proceso de digitalización, así como de las herramientas a utilizar.

El contratista realizará una ficha técnica de cada serie documental digitalizada en que se recoja información del proceso de digitalización: formato, resolución, responsable de la digitalización y fecha de la digitalización.

El Ayuntamiento de Pamplona supervisará la correcta calidad de los documentos digitalizados. Si se ha previsto digitalizar un gran volumen de documentos, se valorará la posibilidad de llevar a cabo una fase de pruebas previas, teniendo en cuenta lo siguiente:

- Antes de iniciar los procesos de digitalización en serie, el contratista deberá realizar una prueba piloto de calidad con una muestra de documentos, a fin de establecer los procedimientos y controles de calidad más adecuados.
- En caso de que se observe alguna incidencia, el contratista y el Ayuntamiento de Pamplona procederán a introducir los cambios necesarios para garantizar la calidad del resultado final.

La certificación de los trabajos dependerá de los controles de calidad de los documentos digitalizados que se realizarán conjuntamente entre el contratista y el Ayuntamiento de Pamplona. Estos controles se basarán en las pautas recogidas en los informes técnicos *UNE-ISO/TR 13028 IN* Información y documentación - directrices para la implementación de la digitalización de documentos (Anexo D: Recomendaciones sobre control de calidad) y *UNE-ISO/TR 15801 IN* Imagen electrónica - Información almacenada electrónicamente - Recomendaciones sobre veracidad y fiabilidad.

En concreto, se establecen los siguientes **controles de calidad**:

1. **Comprobación periódica de los escáneres:** funcionamiento, parámetros de rendimiento, limpieza y mantenimiento.
2. **Registro de los documentos escaneados por sesión:** número de documentos diferenciados y número de unidades de los que consta un documento (más de una página).
3. **Análisis de muestras:** evaluación de una muestra de documentos comparando los resultados del escáner con los parámetros de digitalización establecidos (formato, resolución, compresión, etc.).

4. Calidad de las imágenes:

- Legibilidad de los detalles más pequeños (p. ej., signos de puntuación, comas decimales);
- Completitud de los detalles (p. ej., si los caracteres rotos son aceptables, si faltan segmentos de líneas);
- Exactitud dimensional (comparación con el tamaño del documento original);
- Basuras generadas por el escáner (no presentes en el original);
- Completitud del área total de la imagen (p. ej., si falta información del documento original en los bordes del área de la imagen);
- Densidad de las áreas sólidas negras;
- Fidelidad del color.

5. Metadatos:

- Cumplimiento de las normas establecidas en el proyecto de digitalización;
- procedimientos para admitir documentos digitalizados con metadatos incompletos;
- pertenencia y exactitud de los metadatos;
- ortografía y puntuación (comprobación de que la ortografía y la puntuación sean correctas, especialmente en el caso de los datos introducidos de forma manual);
- coherencia en la creación de metadatos y en su interpretación;
- completitud de los metadatos (comprobación de que todos los campos obligatorios se han rellenado).

6. Verificación de la exactitud del identificador del fichero: los nombres de ficheros deberían identificar de forma consistente y única el documento digitalizado y constar como metadato.

7. Verificación de la secuencia correcta y de la completitud de elementos con diversas páginas: las páginas deberían estar en el orden correcto y no debería faltar ninguna.

Los datos del control de calidad deberían capturarse en un sistema formal ya que pueden tener valor a largo plazo a la hora de tomar futuras decisiones de conservación. Esto puede llevarse a cabo, bien a nivel de archivo, convirtiendo estos datos como parte integral de los metadatos de los documentos digitalizados, bien a nivel de proyecto, manteniendo un diario de control de calidad en el que figuren los resultados de todas las comprobaciones.

Si se detecta que **[más de un 1%]** del número total de imágenes y metadatos asociados examinadas en una muestra seleccionada al azar son defectuosas de acuerdo a los controles de calidad indicados anteriormente, se deberían volver a revisar todos los documentos desde el último control de calidad. Los errores encontrados en el muestreo y

cualquier otro error encontrado en la revisión posterior deberían corregirse volviendo a redigitalizar los documentos sin que ello cause un coste adicional para el Ayuntamiento y sin perjuicio de las acciones contractuales legales a las que esto dé lugar. Estas repeticiones no pueden repercutir en el plazo de ejecución del contrato, si se incurriera en demora injustificada el contratista será penalizado.

Se establece además el siguiente acuerdo de nivel de servicio:

- Se digitalizarán al **[día/semana/mes/trimestre]** menos **[número]** hojas. **[decidir por el Ayuntamiento atendiendo a parámetros de hardware y software]**.
- La repetición de la digitalización derivada de deficiencias en la resolución de la imagen o incumplimiento de los formatos establecidos por el Ayuntamiento de Pamplona deberá realizarse en un plazo inferior a **[número] [días/semanas/meses]**, desde la fecha de notificación de los errores, sin retrasos en el resto de los trabajos a ejecutar.
- La necesidad de rectificaciones en el archivo erróneo o captura por el contratista deberá realizarse en el plazo de **[número] [días/semanas/meses]** desde la fecha de notificación de los errores, sin retrasos en el resto de los trabajos a ejecutar. **[Pendiente de decidir por el Ayuntamiento según el grado de externalización]**.
- Las rectificaciones en los metadatos de los documentos deberán realizarse en el plazo de **[plazo en horas/días/semanas/meses]** desde la fecha de notificación de los errores, sin retrasos en el resto de los trabajos a ejecutar. **[Pendiente de decidir por el Ayuntamiento según el grado de externalización]**.

1.6 Posibilidad o no de subcontratar o ceder a terceros parte del servicio

Pueden darse las siguientes dos posibilidades:

- **No se permite la subcontratación ni la cesión**

No se permite la subcontratación ni la cesión de los servicios objeto del presente contrato.

- **Se permite la subcontratación**

El contratista deberá comunicar anticipadamente y por escrito al Ayuntamiento de Pamplona su intención de subcontratar, con indicación de la identidad del subcontratista, las partes de la prestación que se pretende subcontratar y el porcentaje total de los trabajos a subcontratar en relación a la cuantía total del contrato justificando suficientemente la aptitud de éste para ejecutarla por referencia a los elementos técnicos y humanos de que dispone y a su experiencia.

En cualquier caso, la subcontratación deberá ser aceptada por escrito por el Ayuntamiento de Pamplona y no podrá ser superior al porcentaje del **[porcentaje pendiente de decidir por el Ayuntamiento teniendo en cuenta el límite del TRLCSP]** % del precio del contrato.

Los subcontratistas quedarán obligados sólo ante el contratista, que asumirá la responsabilidad de la ejecución del contrato ante el Ayuntamiento de Pamplona con ajuste estricto a los términos del contrato.

El contratista se obliga a abonar a los subcontratistas y suministradores el pago del precio pactado con unos y otros, en los plazos y condiciones que no sean más desfavorables que las establecidas para las relaciones del Ayuntamiento de Pamplona y el contratista.

El subcontratista no deberá estar incurso en las prohibiciones que según el art. 60 de la TRLCSP prohíben contratar con el Sector Público.

El contratista deberá justificar ante el Ayuntamiento de Pamplona la existencia de la certificación prevista en el art. 43 Ley General Tributaria.

No se permite la cesión del contrato.

1.7 Medidas mínimas según el lugar de prestación del servicio

Pueden darse las siguientes dos posibilidades:

- ***El servicio se presta en las instalaciones del Ayuntamiento de Pamplona***

El servicio debe prestarse en las instalaciones del Ayuntamiento de Pamplona.

Es obligación del contratista optimizar el espacio físico de almacenamiento tanto del servidor como de otros medios usados para este efecto. Se deben evitar duplicidades innecesarias de documentos digitalizados. Se debe respetar el árbol de archivo que se ha acordado con el Ayuntamiento de Pamplona para la captura de la documentación digitalizada.

Se deben establecer normas y procedimientos para la protección adecuada sobre todos los activos del Centro como son la información física (documentos), la información digital (información almacenada) y los medios de producción. Se debe garantizar la trazabilidad de la documentación para conocer la ubicación exacta de los documentos en todo momento.

Sólo tendrá acceso al Centro y a la documentación el personal autorizado del contratista.

- ***El servicio se presta fuera de las instalaciones del Ayuntamiento de Pamplona / El servicio debe prestarse en las instalaciones del contratista.***

El traslado de la documentación es por cuenta y riesgo del contratista, siendo responsabilidad del contratista los daños por el deterioro o extravío de documentación del Ayuntamiento de Pamplona.

Es obligación del contratista optimizar el espacio físico de almacenamiento tanto del servidor como de otros medios usados al efecto del Ayuntamiento de Pamplona. Se deben evitar duplicidades innecesarias de documentos digitalizados. Se debe

respetar el árbol de archivo que se ha acordado con el Ayuntamiento de Pamplona para la captura de la documentación digitalizada.

El contratista debe contar con medidas de seguridad que permitan preservar la confidencialidad, integridad y disponibilidad de la información. Por lo tanto, deberá implementar las siguientes medidas:

- Cumplimiento de la Política de Seguridad del Ayuntamiento.
- La documentación debe guardarse bajo llave y en un recinto seguro de daños por agua para evitar daños y robo de la documentación. El personal que trate la documentación y acceso a los sistemas del Ayuntamiento de Pamplona será el exclusivamente autorizado sin que personas no autorizadas tengan acceso al puesto de trabajo. La documentación deberá estar vigilada con cámaras de seguridad. **[pendiente de decidir por el Ayuntamiento]**
- Se deberá contar en las instalaciones con las medidas de seguridad reglamentariamente establecidas respecto a incendios y riesgos eléctricos.
- Se deben establecer normas y procedimientos para la protección adecuada sobre todos los activos del Centro, la información física (documentos), la información digital (información almacenada) y los medios de producción.
- Se realizarán albaranes de entrada/salida. Cualquier movimiento de documentos entre las instalaciones del cliente y el Centro de digitalización debería estar controlado, previa notificación, mediante un inventario de lotes recogido en el albarán asociado a cada transporte, por duplicado y firmado por ambas partes. Se debe tener la trazabilidad de la documentación, para conocer la ubicación exacta de los documentos en todo momento.
- Se debe informar al personal de que la documentación que tratan tiene carácter confidencial.

1.8 Certificación de la digitalización mediante firma electrónica

En caso de que la digitalización se tenga que realizar en las instalaciones del proveedor, el Ayuntamiento decidirá si el procedimiento de digitalización debe incluir la certificación de las imágenes de los documentos mediante una firma electrónica. En tal caso, la firma electrónica se deberá generar de manera automática, utilizando un certificado digital instalado en el propio sistema de digitalización empleado para digitalizar la documentación del Ayuntamiento de Pamplona quien determinará cuál debe ser el certificado digital que se utilice.

En caso de que el Ayuntamiento de Pamplona exija el uso de un sello electrónico que certifique el proceso automatizado de la digitalización, su aplicación y custodia de certificados atenderá a lo previsto en la Política de Firma Electrónica del Ayuntamiento de

Pamplona que forma parte de su Modelo de Gestión de Documentos Electrónicos y se pondrá a disposición del proveedor al inicio de los trabajos.

1.9 Penalizaciones

Para la realización de los trabajos se realizará un seguimiento de la evolución de las actuaciones que quedará reflejado en los informes de seguimiento y con el fin de corregir desviaciones que pudieran afectar al resultado final de los trabajos.

A efectos contractuales se considerará falta penalizable toda acción u omisión del contratista que suponga una ruptura de las exigencias específicas en el contrato.

Los defectos en que incurra el contratista en la ejecución del contrato, aunque no proceda por ello la resolución del mismo, darán lugar a la amonestación por escrito por parte del Ayuntamiento de Pamplona al Contratista.

Las penalizaciones podrán recaer sobre las siguientes circunstancias o elementos:

- a. Demora del contratista en inicio de los trabajos.
- b. Demora en la ejecución de los servicios del contrato.
- c. Demora en la incorporación del equipo de trabajo o de los medios personales asignados para su sustitución.
- d. Incumplimiento del procedimiento de sustitución de medios personales. (En caso de que se haya establecido en el pliego un procedimiento para la sustitución).
- e. Calidad del servicio:
 - Por incumplimiento de los objetivos planificados o por cumplimiento defectuoso del servicio imputables al contratista, por falta de responsabilidad, incompetencia, negligencia u otras causas de índole similar.
 - Por incumplimiento que dé lugar a baja en el rendimiento convenido de acuerdo con el nivel de servicio acordado.
- f. Incumplimiento de las condiciones establecidas para proceder a la subcontratación, no acredite la aptitud del subcontratista o de las circunstancias determinantes de la situación de emergencia o de las que hacen urgente la subcontratación.

Las penalizaciones a aplicar serán las siguientes:

1. Penalización **[diaria/mensual/trimestral/semestral/anual]**de **[importe]** €
2. **[PENALIZACIÓN de un porcentaje del precio].**
3. **[PENALIZACIÓN de un porcentaje de la facturación mensual].**

En caso de mantenerse o reiterarse la defectuosa ejecución del contrato tras **[incluir número de amonestaciones]** amonestaciones por escrito, el Ayuntamiento de Pamplona procederá a la resolución del contrato.

Las penalizaciones se deducirán por el Ayuntamiento de Pamplona en hacer efectivo el abono correspondiente.

La aplicación y pago de estas penalizaciones no excluye la indemnización a la que el Ayuntamiento pueda tener derecho por daños y perjuicios causados por retrasos o incumplimientos imputables al contratista.

En el caso de existir garantía, esta responderá de la efectividad de aquéllas, cuando no puedan deducirse de los documentos de pago al contratista.

1.10 Responsabilidad del contratista por daños y perjuicios

El contratista ejecutará el contrato en los términos previstos, realizando de manera competente y profesional el objeto del contrato, cumpliendo los niveles de calidad exigidos y cuidando diligentemente los equipos y espacios físicos del Ayuntamiento de Pamplona que tuviera que utilizar como consecuencia del contrato. A estos efectos, el contratista responderá de la calidad del trabajo desarrollado con la diligencia exigible a una empresa experta en la realización de las actividades del tipo del objeto del contrato.

El contratista responderá de la corrección y precisión de los servicios e informes que aporte en ejecución del contrato y avisará sin dilación al Ayuntamiento de Pamplona cuando detecte un error para que pueda adoptar las medidas y acciones correctoras que estime oportunas.

El contratista responderá de los daños y perjuicios que se deriven para el Ayuntamiento de Pamplona, o para el personal de la misma, de las reclamaciones que pueda realizar un tercero, y que tengan su causa, directa o indirecta, en errores, métodos inadecuados o conclusiones incorrectas del contratista, o de su personal, en la ejecución del contrato o que deriven de la falta de diligencia referida en el presente apartado.

El contratista responderá por cualquier daño directo que pudiera resultar del incumplimiento de las obligaciones de confidencialidad previstas en el presente contrato.

El contratista es responsable del cuidado y custodia de la documentación entregada por el Ayuntamiento debiendo establecer medios de seguridad y conservación de los originales que deberán ser devueltos organizados en el mismo estado en que fueron entregados sin que hayan sufrido ningún tipo de alteración, o modificación en su presentación o contenido.

Es responsabilidad del contratista realizar las instalaciones y configuraciones de los equipos o elementos informáticos que necesite para montar su infraestructura de trabajo. Igualmente, los rendimientos de ello son su responsabilidad, así como el soporte, mantenimiento, actualizaciones y licencias de software que se tengan que realizar.

[Depende del alcance del contrato y de la propiedad de las herramientas a utilizar si son del contratista o del Ayuntamiento].

No se pueden emplear herramientas que contengan malware, virus o que de otra manera estén comprometidas y que puedan infectar material del Ayuntamiento de Pamplona o dañar los datos contenidos en los sistemas de almacenamiento del Ayuntamiento de

Pamplona. Si se comprobara este daño éste deberá ser reparado por el contratista sin perjuicio del derecho del Ayuntamiento de Pamplona a ejercitar los derechos que le pudieran corresponder. **[Depende del alcance del contrato y de la propiedad de las herramientas a utilizar si son del contratista o del Ayuntamiento].**

1.11 Garantía

El contratista se obliga a prestar garantía de forma expresa en los cinco días siguientes a la adjudicación, por el importe del 5% del importe del contrato, para asegurar el correcto funcionamiento de los trabajos realizados en ejecución del contrato, y se mantendrá durante el plazo de **[número]** meses a contar desde la fecha de su finalización, obligándose a realizar, sin coste para el Ayuntamiento de Pamplona y durante este tiempo, las correcciones y modificaciones necesarias para subsanar los errores que eventualmente pudieran aparecer.

La garantía podrá constituirse mediante depósito, seguro de caución o aval.

En caso de que se hagan efectivas sobre la garantía las penalidades o indemnizaciones exigibles al contratista, éste deberá reponer o ampliar aquélla, en la cuantía que corresponda, en el plazo de quince días desde la ejecución, incurriendo en caso contrario en causa de resolución.

La garantía responderá de los siguientes conceptos:

- De las penalidades impuestas al contratista.
- De la correcta ejecución de las prestaciones contempladas en el contrato, de los gastos originados al Ayuntamiento de Pamplona por la demora del contratista en el cumplimiento de sus obligaciones y de los daños y perjuicios ocasionados a la misma con motivo de la ejecución del contrato o por su incumplimiento, cuando no proceda su resolución.
- De la incautación que puede decretarse en los casos de resolución del contrato, de acuerdo con lo que en el mismo o en la Ley esté establecido.

1.12 Jurisdicción

El presente contrato tiene naturaleza administrativa siendo competencia de la Jurisdicción Contencioso Administrativa resolver las cuestiones litigiosas que surjan respecto de la interpretación, ejecución, modificación y resolución del contrato.

1.13 Resolución

El contratista podrá resolver el contrato, con derecho a la indemnización de daños y perjuicios causados, si el contratista no cumple las obligaciones contempladas en el mismo.

Son causas de resolución del contrato:

- La muerte o incapacidad sobrevenida del contratista individual o la extinción de la personalidad jurídica de la sociedad contratista. En los casos de fusión de empresas en las que participe la sociedad contratista, continuará el contrato vigente con la entidad absorbente o con la resultante de la fusión, que quedará subrogada en todos los derechos y obligaciones procedentes del mismo. Igualmente, en los supuestos de escisión, aportación o transmisión de empresas o ramas de actividad de las mismas, continuará el contrato con la entidad resultante o beneficiaria, que quedará subrogada en los derechos y obligaciones procedentes del mismo, siempre que tenga la solvencia exigida al acordarse la adjudicación.
- La declaración de concurso o la declaración de insolvencia en cualquier otro procedimiento.
- El mutuo acuerdo entre las partes.
- La no formalización del contrato en plazo.
- La demora en el cumplimiento de los plazos por parte del contratista, el incumplimiento de los plazos o las obligaciones esenciales establecidas en el contrato y no conseguir los objetivos por causas imputables al contratista.
- Cualquier tipo de incumplimiento después de la **[indicar número]** amonestación.
- La falta de capacidad o solvencia sobrevenida o estar acometiendo, con posterioridad a la adjudicación, en alguna de las prohibiciones de contratar.
- Las demás establecidas expresamente en el contrato.

En caso de resolución del contrato, el contratista, a solicitud del Ayuntamiento, deberá cesar inmediatamente en todos los trabajos contratados. Asimismo, se procederá a efectuar la liquidación definitiva de los trabajos realizados hasta la fecha que se consideren útiles para el Ayuntamiento de Pamplona, la que abonará los trabajos realizados en las condiciones establecidas en el contrato hasta esa fecha. En todo caso, el Ayuntamiento de Pamplona deducirá de la cantidad que resulte de la liquidación del importe correspondiente a indemnizaciones y otros conceptos que procedan.

La resolución del contrato se acordará por el órgano de contratación del Ayuntamiento.